ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA ELEKTROTECHNICKÁ

KATEDRA TECHNOLOGIÍ A MĚŘENÍ

BAKALÁŘSKÁ PRÁCE

Bezpečnost IoT

Vojtěch Topinka **2019**

Zadání BP

Abstrakt

Předkládaná bakalářská práce se zabývá problematikou bezpečností v systémech IoT. Má za úkol informovat o riziku, které sebou nese používání takovýchto systémů. První kapitola této práce se věnuje seznámení s pojmem internet věcí. Jsou zde základní informace o architektuře, principu, dnešním využití internetu věcí a také popisuje některé používané komunikační sítě. V druhé časti je vysvětlena bezpečnost internetu věcí. IoT systém je rozdělen podle obecné architektury a v každé vrstvě jsou popsány informace týkající se bezpečnosti. Dále jsou vysvětleny útoky na fyzická zařízení a také opatření, které mají těmto útokům předcházet. Ve třetí kapitole jsou uvedeny útoky na IoT zařízení, které se ve světě staly. V poslední části je celkové zhodnocení této problematiky.

Klíčová slova

IoT, Bezpečnost, Internet věcí, útoky na IoT, Kybernetická bezpečnost

Abstract

This bachelor thesis deals with security issues in IoT systems. Its task is to inform about the risk of using these systems. The first chapter of this work deals with the concept of the Internet of Things. There are basic information about architecture, principle, today's use of Internet of Things and also describes some used communication networks. The second part explains the security of the Internet of Things. The IoT system is structured according to general architecture and security information is described in each layer. Furthermore, attacks on physical devices are explained as well as measures to prevent these attacks. In the third chapter, there are attacks on IoT devices that have happened in the world. The last part is an overall evaluation of this issue.

Key words

IoT, Security, Internet of things, Attacks on IoT, Cyber security

Prohlášení

Prohlašuji, že jsem tuto diplomovou/bakalářskou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

Dále prohlašuji, že veškerý software, použitý při řešení této bakalářské/diplomové práce, je legální.

.....

podpis

V Plzni dne 21.8.2019 Vojtěch Topinka

Poděkování

Tímto bych rád poděkoval vedoucímu bakalářské práce panu Ing. Karlu Šímovi, za poskytnuté rady a za vstřícné vedení mé bakalářské práce.

Obsah

Úvod

Dnes je internet věcí velice diskutované a rychle se rozvíjející téma. Využívá se ve spoustě odvětví, od domácností po těžký průmysl. Ve své nejjednodušší podobě je internet věcí myšlenka, že bezdrátová komunikace a digitální inteligence mohou být zabudovány do všeho kolem nás, ať už jde o nositelnou elektroniku, vozidla, budovy, stroje atd.. Základem této koncepce je spojení fyzické, digitální a lidské infrastruktury, které umožní miliardám zařízení shromažďovat, přenášet a zpracovávat data s využitím internetu. Systémy internetu věcí umožňují uživatelům dosáhnout větší stupeň automatizace, lépe a rychleji analyzovat data a na základě toho následně rychleji a lépe reagovat na určité situace. Dnes jsou tyto systémy také hojně používané ve zdravotnictví, pomáhají zlepšit zdravotní péči v nemocnicích a umožňují sledování životních funkcí. Bohužel internet věcí s sebou přináší také určitá rizika. Některé aplikace internetu věcí zatím nenabízí dostatečné zabezpečení. Je tomu tak například u zařízení s nižším výkonem, a malému výpočetnímu výkonu informačního systému. V těchto případech mají často systémy velmi slabé zabezpečení a případný útok je většinou úspěšný. To může zapříčinit zničení zařízení, nebo únik soukromých informací. Ty mohou být jakýmkoliv způsobem zneužita. Například může jít o informace s politickým podtextem, ale také to mohou být informace k finančním účtům, nebo obyčejné fotografie. V každém případě je třeba se těmto rizikům věnovat a aplikovat dostatečné bezpečnostní opatření do systémů internetu věcí.

Seznam symbolů a zkratek

CoAP ..... Constrained application protocol

DNS ..... Domain name systém

DoS ..... Denial of Service

EKG ..... Elektrokardiografie

GPS ..... Global positioning system

GSM ..... Global system for mobile

IoT ..... Internet of Things – Internet věcí

IMD ..... Implentable medical devices

IP ..... Internet protocol

LTE ..... Long term evolution

MQTT ..... Message queuing telemetry transport

NFC ..... Near field communication

PaaS ..... Platform as a Service

RFID ..... Radio frequency identification

SaaS ..... Software as a Service

SITMP ..... Správa informačních technologií města Plzně

SNR ..... Signal to Noise ratio

WSN ..... Wireless sensor network

WiFi ..... Wireless fidelity

1 IoT

1.1 Historie

Pojem „Internet of Things“ poprvé použil tehdejší výkonný ředitel společnosti Auto-ID center jako název své prezentace pro Procter & Gamble v roce 1999 [1]. Hlavní myšlenkou tehdy bylo využití RFID v dodavatelském řetězci P & G.

Jako první IoT zařízení lze považovat toustovač Johna Romkeye. John Romkey v roce 1990 svůj toustovač propojil s internetem za účelem ovládání.

Podle internetové služby Cisco Internet Business Solution Group se ale internet věcí oficiálně narodil až 2008 až 2009 v okamžiku, kdy bylo k internetu připojeno více zařízení, než bylo na světě lidí [2]. Není třeba dodávat, že dnes je počet takovýchto zařízení mnohonásobně vyšší. Existuje mnoho studií [3][4], které předpovídají, jak se bude vyvíjet počet připojených IoT. Čísla se samozřejmě liší, ale jedno mají všechny studie společné: předpovídají v následujících pěti až deseti letech velký IoT zařízení.

1.2 Princip

Hlavní myšlenkou internetu věcí (Internet of Things) je bezdrátové propojení „věcí“ v podobě senzorů, čidel a různých elektronických zařízení, které mezi sebou komunikují a navzájem se ovlivňují. Sbírají tak informace, které jsou dále vyhodnocovány, a dále se s nimi pracuje.

Kompletní systém IoT integruje tedy čtyři odlišné komponenty: senzory (koncová zařízení pro sběr dat), konektivitu, zpracování dat a uživatelské rozhraní [5].

- Senzory a zařízení

Jedná se o koncová zařízení, která zprostředkovávají měřicí data. Nejčastěji se jedná o senzorová zařízení nebo běžná zařízení zasílající například telemetrická data a informace o svém chodu. Koncové zařízení může být jednoduché – jednoúčelové. Například se může jednat o snímání teploty v místnosti, anebo se může jednat o komplexnější zařízení, které například využívá nejmodernější poznatky z oblasti umělé inteligence a ze živého obrazového streamu rozeznávat například nějaké objekty nebo stavy. Samozřejmě je možné využívat více snímačů paralelně, nebo se může jednat o koncová zařízení, která jsou součástí jiného zařízení, které snímá více údajů současně. Jako hlavní cíl koncového zařízení IoT lze označit sběr informací.

- Připojení

Nasbíraná data jsou následně odesílány do nějakého informačního systému. V současné době je velké množství technologií jak přenést informace z koncového zařízení právě do nějakého informačního systému internetu věcí. Nejčastěji se může jednat o ethernetové připojení, WiFi, ZigBee, nízko výkonové bezdrátové sítě pro IoT (LPWAN – Low Power Wide Area Network). Při volbě způsobu přenosu informací musíme uvažovat spotřebu energie, šířku pásma, vzdálenost přenosu a rušení v dané oblasti. Technologii připojení volíme podle konkrétní aplikace IoT.

- Zpracování dat

Jak bylo zmíněno, data jsou přenášena z koncového zařízení skzre nějaké připojení do IoT informačního systému. V dnešní době je velmi populární trend využívaní cloudových služeb. Nejběžnější zprostředkování cloudových služeb je typu: SaaS (Software as a Service – poskytování softwaru jako služba), PaaS (Platform as a Service – poskytování platformy jako služba) a IaaS (Infrastructre as a Service – poskytování celé infrastruktury jako služba). Z toho je patrné že cloudové služby jsou o poskytování běžných prostředků informatiky ale jako služba – tedy dodání konkrétních prostředků na klíč. V současné době takto poskytuje IT prostředny například: Microsoft – MS Azure, IBM – IBM BlueMix, Amazon – AWS (Amazon Web Services).

Po přenosu dat skrze konkrétní přenosovou technologii se data dostanou do daného informačního systému. V tomto systému se data pomocí určitého programu/služby zpracovávají. Tato činnost může být velice jednoduchá, jako například porovnání zjištěné teploty s mezní hodnotou nebo se může jednat o nějaké pokročilejší operace. Datové informační systém může například provádět agregaci dat, filtraci dat, sledování a odhad trendu daných dat atd. Po vyhodnocení dat informační systém může připravit například časový report nebo může identifikovat a notifikovat nějakého nestandartního chování a tím se dostáváme k uživateli, který například musí rozhodnout, jaké budou například další kroky.

- Uživatelské rozhraní

Pokud tedy informační systém vyhodnotí data, je nutné je prostředkovat nějakou formou cílovému uživateli. Nejčastěji se může jednat o nějaké výstupní tiskové sestavy, nebo grafické sestavy reprezentující data. Toto ve většině případů náleží uživatelskému rozhraní danného IoT systému. Uživatelské rozhraní totiž zobrazuje a vizualizuje data

konečnému uživateli. Uživatel následně může rozhodovat, jak s nimi naloží. Například když systém na bezpečnostní kameře rozpozná osoby, či objekty, které mohou představovat hrozbu, informují majitele systému, případně příslušné orgány. Některé akce se mohou ale provádět automaticky již v daném systému. Například když se teplota v budově automaticky reguluje pomocí termostatu a uživatel skrze uživatelské rozhraní je informován a může provést kontrolu, případně upravit parametry následkem změny požadavků/preference.

1.3 Vize internetu věcí

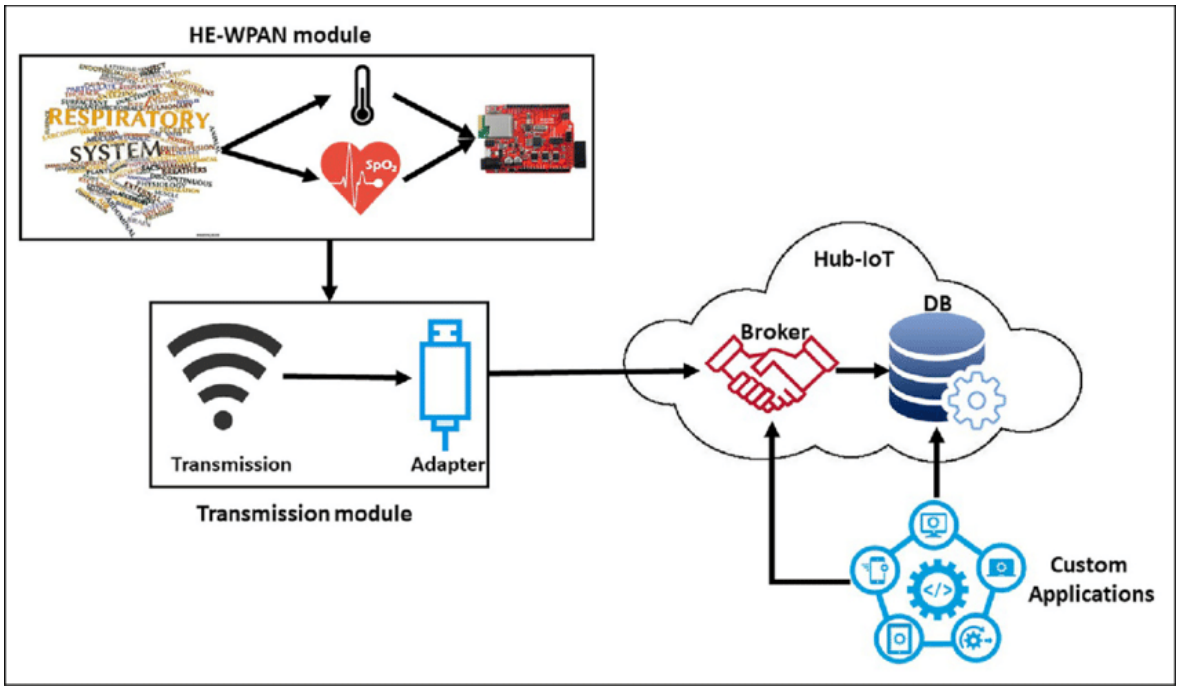
V poslední době se začíná objevovat pojem Internet of Everything (IoE), což v překladu znamená internet všeho. Od internetu věcí se odlišuje hlavně myšlenkou na inteligentnější propojení věcí. Spíše než komunikace fyzických objektů je využívána umělá inteligence, aby se všechny koncepty spojily do jednotnějšího systému. Příklad uvedený
v [6] vysvětluje rozdíl mezi IoE a IoT na příkladu železniční tratě. Samotnou železniční trať v podobě kolejí přirovnává k internetu věcí a internet všeho přirovnává ke všem součástím železniční tratě, kam patří koleje, samotné vlaky, automaty na lístky, personál železnice atd..

Dnes je IoE se považuje za nadmnožinu IoT a společnost Cisco, která poprvé použila pojem Internet všeho, se domnívá, že propojením lidí, dat, procesů a „věcí“ aplikace internetu věcí stanou relevantnějšími a hodnotnějšími.

Největší dopad této myšlenky se předpokládá v oblasti průmyslu a podnikání [7]. Příkladem může být nositelná elektronika a například společnost Google se zabývá autonomní dopravou, která se zdá být v poslední době více reálná. Dalšími oblastmi, kde se předpokládá využití technologie IoE jsou pokročilá lékařská zařízení, automatizované továrny, zemědělské stroje atd.. Ale stále nesmíme zapomínat na bezpečnost, jelikož více zařízení znamená více dat a přenášených informací, ale také větší obavy o soukromí a zabezpečení dat.

1.4 Architektura

Podle [8], [9] je obecná architektura IoT složená ze tří základních vrstev. Jsou to aplikační, transportní a snímací. Každá vrstva je zde definována tak, aby vykonávala konkrétní úkol a funkci, ke kterému je určená.



Obr. 1 Obecná architektura IoT

Převzato z: [10]

1.4.1 Senzorická vrstva

Vrstva senzorická má za úkol shromažďovat informace v reálném čase. To provádí pomocí senzorových jednotek, které sbírají informace v podobě měření různých veličin např.: teplota, osvětlení, vlhkost, zvuk, síla atd..

1.4.2 Transportní vrstva

V této vrstvě jde především o směrování komunikace a přenos všech informací. Většinou se jedná o end-to-end komunikaci a měla by zajišťovat spolehlivost, bezpečnost dat, a správné pořadí odeslaných paketů. Komunikace může být zprostředkována různými technologiemi, podle konkrétní aplikace internetu věcí. Přenosové sítě můžeme rozdělit na kabelové a bezdrátové a dále podle vzdálenosti.

1.4.2.1 Kabelová komunikace

Kabelové připojení poskytuje velmi spolehlivou komunikaci, kterou je možné využít mezi stroji ve výrobních halách nebo například k propojení zařízení ve firemních kancelářích. Rozšíření sítě lze dosáhnout například použitím průmyslových směrovačů pro zajištění bezpečné, spolehlivé a vysokorychlostní komunikace [11]. U fyzicky připojeného zařízení je méně pravděpodobné rušení a to přispívá k větší spolehlivosti sítě. Použitím

kabelových sítí lze často přenášet více dat za nižší náklady nežli například bezdrátové mobilní datové služby.

Ethernet

Jde o technologii vyvinutou v 70. letech 20. století a používal se pro komunikaci v LAN sítích. Díky dnešním technologiím se již ethernet může využívat i v sítích MAN. Dnes se používají pro přenos speciální kroucené kabely využívající výhody kroucená dvojlinky a stínění, nebo optická vlákna. Dříve se využívali i koaxiálním kabely, ty ale vzhledem ke svým nedostatkům byly nahrazeny kroucenými a optickými kabely[12]. Pro přenosu dat touto technologií je potřeba minimálně propojovací prvek (ethernetový kabel, optický kabel) a aktivní síťové prvky (rozbočovač, přepínač a směrovač) [13]. V porovnání s bezdrátovými technologiemi je kabelový přenos dat stabilnější, protože na něj nepůsobí tolik rušivých vlivů. Má také menší latenci. Má vyšší přenosovou rychlost a běžně se využívají standardy 10 Gbit/s, 40 Gbit/s a 100 Gbit/s [14].

1.4.2.2 Wireless Local-Area Network –WLAN

Jde o bezdrátové sítě s krátkým dosahem, které se využívají pro komunikaci hlavně v domácnostech, firmách, školách a jiných budovách.

- Wi-fi

Tato technologie je dnes používaná běžně v každé domácnosti, jako možnost bezdrátového připojení k internetu. Je tedy možné ji využívat k přenosu informací v oblasti IoT. Standartní používaná Wi-fi má dosah v řádu desítek metrů a frekvenční rozsah 2,4 – 60 GHz.

V roce 2017 byl představen nový síťový protokol nazývaný Wi-Fi HaLow, který pracuje v pásmu 900MHz a disponuje menší spotřebou energie [15]. Je tedy vhodný pro připojení velkých skupin zařízení a senzorů, což je při používání IoT systémů potřeba.

- Z-Wave

Jde o nízkoenergetickou radio frekvenční komunikační technologii určenou k připojení domácích spotřebičů [16]. Například se touto technologií připojují regulátory osvětlení a různé senzory. Tato technologie je spolehlivá, pro potřeby IoT má i relativně malou přenosovou rychlost (do100kbit/s) a komunikuje s nízkou latencí. Pracuje v pásmu okolo 1GHz, takže může fungovat zároveň s WiFi, nebo Bluetooth bez vzájemného rušení. Je velmi škálovatelná, což umožňuje připojení až 200 zařízení. Hlavní nevýhoda je pouze

jediný výrobce komunikačních čipů pro tuto technologii, kterým je Sgma designes.

- ZigBee

Tato síť je vhodná pro připojení zařízení, která přenáší malé množství dat v uzavřeném systému [17]. Používá se například při automatizaci spotřebičů v domácnosti a výhodou je nízká energetická náročnost, dosah až 100 metrů a spolehlivost.

1.4.2.3 Low-Power Wide-Area Network – LPWAN

Jedná se o komunikační sítě s velkým dosahem v řádech desítek kilometrů. Tyto sítě jsou určené především pro zařízení s nízkou spotřebou. Z pohledu zasílání dat se jedná o technologie vhodné pro zasílání malého objemu dat na velkou vzdálenost. Zařízení komunikující po těchto technologií jsou z velké části napájeny akumulátory. Nejvíce známé sitě typu LPWAN jsou LoRa a Sigfox, které využívají pouze nelicencované frekvenční pásma, a dále pak síť NB-IoT, která využívá část licencovaného frekvenčního pásma mobilní sítě 4G.

- LoRa

Jedná se o zkratku slovního spojení Long Range. Tento telekomunikační systém má dlouhý dosah (15km), nízkou spotřebou ale také nízkou přenosovou rychlostí. Pro IoT aplikace, ale nízká přenosová rychlost není problémem. Všechny připojené zařízení komunikují s bránami (gateways), které jsou připojené k internetu. Tyto brány tedy přijímají data skrze technologii LoRa a následně data odesílají do centrálního síťového serveru skrze standartní internetové připojení [18]. Tato technologie se využívá hlavně v oblasti Smart city. Příkladem je využívání a rozvoj sítě LoRa v Plzni.

Tato technologie se tedy využívá i u nás v Česku. V roce 2018 již byla pokryta většina republiky [19] a byla vybrána ČRA (České Radiokomunikace) pro vybudování sítě internetu věcí v ČR [20]. Tato technologie využívá frekvenční pásmo 433.05 - 434.79 MHz pro kanál EU433 a 863 - 870 MHz pro kanály EU863-870 [21]. Síť LoRa využívá CSS modulaci.

Republikový lídr v LoRa je společností ČRA, která vybudovala právě sítě pro internet věcí LoRa a pokryla prakticky celou republiku. [22].

V Plzni byla v roce 2017 zprovozněna síť IoT společností SITMP na platformě LoRaWAN [23], která má sloužit městským organizacím k vytvoření IoT infrastruktury.

Tato technologie může být konfigurována pro použití různých přenosových výkonů, nosných frekvencí, rozptylových fraktorů, šířky pásma a kódovací rychlosti [24].

Přenosový výkon může být nastaven od -4dBm do 20 dBm v krocích po 1 dB, ale díky limitům hardwaru je většinou rozsah omezen na 2 – 20 dBm. Také horní hranici přenosového výkonu ovlivňují hardwarové omezení. Výkon nad 17 dBm lze používat pouze v 1% pracovního cyklu.

Frekvence nosiče lze naprogramovat po 61 Hz krocích od 137 MHz do 1020 MHz.

Faktor šíření je poměr mezi rychlostí symbolu a rychlostí čipu. Vyšší faktor šíření zvyšuje poměr signál/šum (SNR) a tím i citlivost a rozsah. Také zvyšuje dobu přenosu paketů. Větší šířka přenosového pásma umožňuje vyšší přenosovou rychlost, ale zároveň nižší citlivost

- Sigfox

Tato síť byla jako první technologie určená primárně pro IoT. V dnešní době pokrývá téměř celou Evropu a rozšiřuje se i v jiných částech světa. Společnost Sigfox tvrdí, že každá brána dokáže spolupracovat až s milionem připojených zařízení v okruhu do 50 kilometrů ve venkovských oblastech a do 10 kilometrů ve městech [25]. Při výstavbě této sítě se využívají již postavené vysílače, které jsou většinou určené pro mobilní komunikaci.

Jedná se o síť s velmi nízkou energetickou náročností, ale také s velmi malou přenosovou rychlostí (cca 100 bitů za sekundu). Zmíněná nízká energetická náročnost je hlavní výhodou, a umožňuje návrh zařízení, která jsou napájené bateriemi s životností, až deset let. Z tohoto důvodu je tato síť velmi vhodná pro IoT.

Tato síť má ale i své uskalí. Připojená zařízení mohou vysílat přibližně 140 zpráv denně [26], to odpovídá 1 zpráva za 10 minut. Mobilní operátor T-mobile a společnost Simple Cell networks tuto síť provozují v České Republice [27].

Sigfox používá pro přenos zpráv frekvenční pásmo 868/902MHz. Jako modulaci využívá Ultra-Narrow band a každá zpráva je široká 100 Hz. Přenosová rychlost je 100 až 600 bitů za sekundu v závislosti na oblasti [28].

- NB-IoT

Jde o úzkopásmovou síť, která může koexistovat s mobilními sítěmi (GSM a LTE) v licencovaných frekvenčních pásmech (700MHz, 800MHz, 900MHz). Může pracovat

ve třech provozních režimech. V prvním případě využívá k přenosu právě používané frekvenční pásma GSM. Dále může vyžívat nevyužité pásma v ochranném LTE pásmu, nebo zdrojové bloky v LTE [29].

V současné době je touto sítí pokryta celá Česká Republika a poskytují ji operátoři O2 a Vodafone [30], [31]. Tato síť používá QPSK modulaci a šířka pásma je 180 KHz [22].

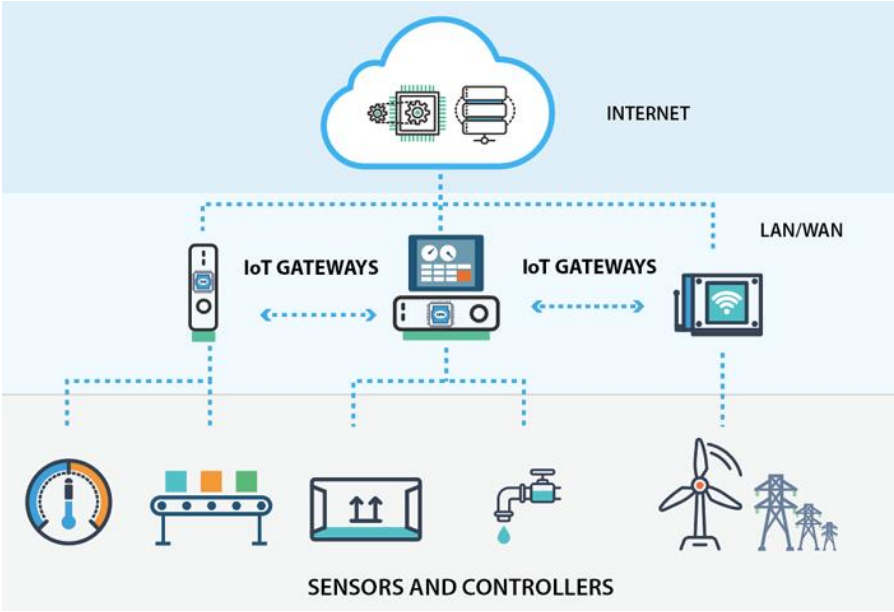
Celulární sítě

Další technologie, které se využívají pro přenos informací v IoT systémech jsou celulární sítě jako GSM, EDGE, 3G a 4G LTE. Tyto sítě se primárně využívají pro mobilní a datovou komunikaci, ale lze je využít i pro připojení zařízení pro internet věcí. Pracují v licencovaných pásmech a jsou schopné přenášet velký objem dat [32], na rozdíl od LPWA a hlavní výhodou je jejich již existující infrastruktura.

Nová generace mobilních sítí nesoucí název 5G je nyní v testovací fázi nasazena v Jižní Korei. 5G slibuje mnohem větší přenosovou rychlost a až desetkrát větší pokrytí. Síť 5G by měla být také velkou změnu i pro oblasti IoT a to především kvůli pokrytí a přenosové rychlosti [33]. V současné době ale ještě není 5G tak rozšířené, aby se mohlo pro účely IoT využívat.

1.4.2.4 Gateway

Gateway, neboli v překladu brána, slouží v infrastrukturách internetu věcí ke komunikaci jednotlivých zařízení mezi sebou, nebo například mezi zařízením a cloudem. Jedná se o hardwarové zařízení, ve kterém pracuje software a jeho primární úlohou je směrování dat. V Případech, kdy senzory generují velké množství dat, může brána sloužit k předběžnému zpracování a filtrování dat [34]. To napomáhá snadnějšímu přenosu a následnému zpracování dat v cloudu. [35]. Pracuje také jako administrátorské rozhraní, kde se mohou provádět základní funkce systému.



Obr. 2 IoT gateway komunikace

Převzato z: [35]

V sítích LoRaWAN jsou brány využívány jako směrovače pro přenos zpráv mezi koncovými zařízeními a centrálním síťovým serverem. Brány jsou připojeny k serverům prostřednictvím běžného IP, zatímco koncová zařízení jsou s bránou propojeny bezdrátovou komunikací [36].

1.4.3 Aplikační vrstva

Aplikační vrstva přijímá data přenášená ze síťové vrstvy a používá je k poskytování požadovaných služeb, nebo operací. Například může poskytovat službu úložiště pro zálohování přijatých dat do databáze, nebo analytickou službu pro vyhodnocení přijatých dat pro predikci budoucího stavu fyzických zařízení. V této vrstvě existuje řada aplikací, z nichž každá má odlišné požadavky.

1.4.3.1 Cloud

Jako jednu z prvních definic, co je to vlastně cloud, představil Buyya et al. V roce 2009 a podle [37] její volný překlad zní: „Cloud je typ paralelního a distribuovaného systému skládajícího se ze sady vzájemně propojených a virtualizovaných počítačů, které jsou dynamicky poskytovány a prezentovány jako jeden nebo více sjednocených výpočetních zdrojů, založených na dohodě požadované a nabízené služby mezi poskytovatelem a spotřebitelem“.

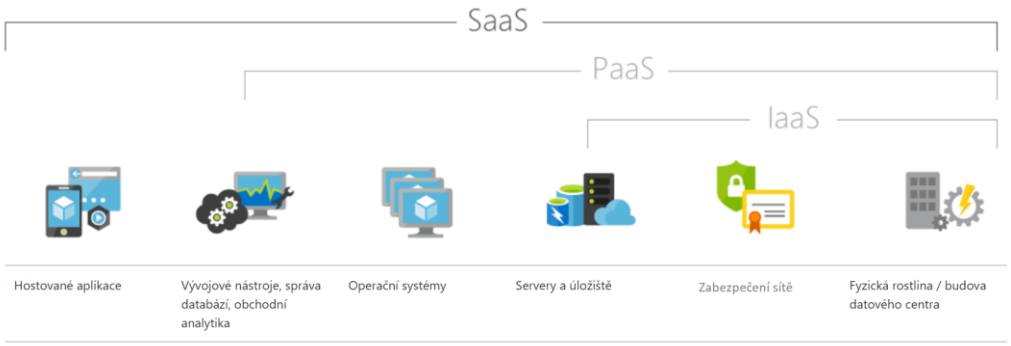
Cloud je obrovská propojená síť výkonných serverů, kterou mohou využívat společnosti i obyčejní lidé. Vzhledem k dnešnímu vysokorychlostnímu připojení je běžné, že místo drahého hardwaru, který by vyhodnocoval data IoT aplikací, se využívají pronajaté cloudové prostředky [38]. Ty odvádějí stejnou práci jako běžný harware, ale jejich použitím ušetříme pořizovací náklady za výpočetní techniku. Obecně můžeme říci, že jakákoliv činnost, která se děje přes internet a neděje se na našem zařízení se děje „v cloudu".

Ne vždy je ale použití cloudu efektivnější řešení. Například společnost Mozilla nabízí produkt Things Gateway, který umožňuje realizovat chytrou domácnost bez použití cloudu. Místo cloudu je v systému takovéto chytré domácnosti využíván Raspberry Pi, který slouží jako mozek celého systému [39]. Jde o tedy o připojení všech zařízení na společnou bránu, která všechny zařízení propojuje a také ovládá.

Tím jak se IoT vyvíjí a stává se komplexnějším, jsou cloudová řešení více využívány ke správě dat. Může se zdát, že systémy IoT automaticky spolupracují s cloudovými datacentry a vytvářejí tak jednotnou strukturu. Ale není tomu tak, jelikož jednotlivé IoT infrastruktury jsou stálé rozdílné a poskytovatelé cloudových služeb se snaží svoje produkty přizpůsobit různým infrastrukturám.[40]. Je to proto, že senzory, brány, a jiná používaná jsou vyvíjeny nezávislena cloudových službách. Můžou se tak lišit například v komunikačních protokolech, nebo jiných aspektech.

Podle [41] rozlišujeme tři základní typy cloudových služeb:

1. Infrastruktura jako služba (IaaS) – jde o pronájem IT infrastruktury včetně serverů, virtuálních zařízení, nebo úložiště.
2. Platforma jako služba (PaaS) – využíváním služby PaaS, kterou nabízí například společnost Microsoft [42], se uživatelům dostává kompletní prostředí umožňující jednoduché cloudové aplikace, ale i složité podnikové aplikace. Paas je nadmnožina služby IaaS a navíc poskytuje middleware, vývojářské nástroje, službu bussines inteligence a správu databází
3. Software jako služba (SaaS) – je další služba, kterou nabízí společnost Microsoft. Oproti službě PaaS navíc obsahuje hostované aplikace. Veškerou podpůrnou infrastrukturu spravuje Microsoft a vše je umístěno v jejich datovém centru.



Obr. 3 Cloudové služby

Převzato z: [43]

V současné době nabízí pronájem cloudových služeb vícero společností. Mezi největší patří již zmíněný Microsoft [44], který nabízí spoustu produktů pro internet věcí, jako je například Azure IoT Central, což je služba umožňující monitoring a správu veškerých zařízení dané aplikace internetu věcí. Další jsou služby, jako Azure IoT Hub, která umožňuje obousměrnou a zabezpečenou komunikaci, mezi IoT aplikací a zařízeními, které spravuje, nebo Azure Stream Analytics zabývající se zpracováním dat velkého počtu připojených zařízení v reálném čas.

Také společnost Amazon nabízí mnoho produktů pro aplikace internetu věcí [45]. Například služba AWS IoT Device Defender, která se se stará o zabezpečení veškerých zařízení dané aplikace, nebo AWS IoT Core, což je cloudová služba.

1.5 Využití

1.5.1 Domácnosti

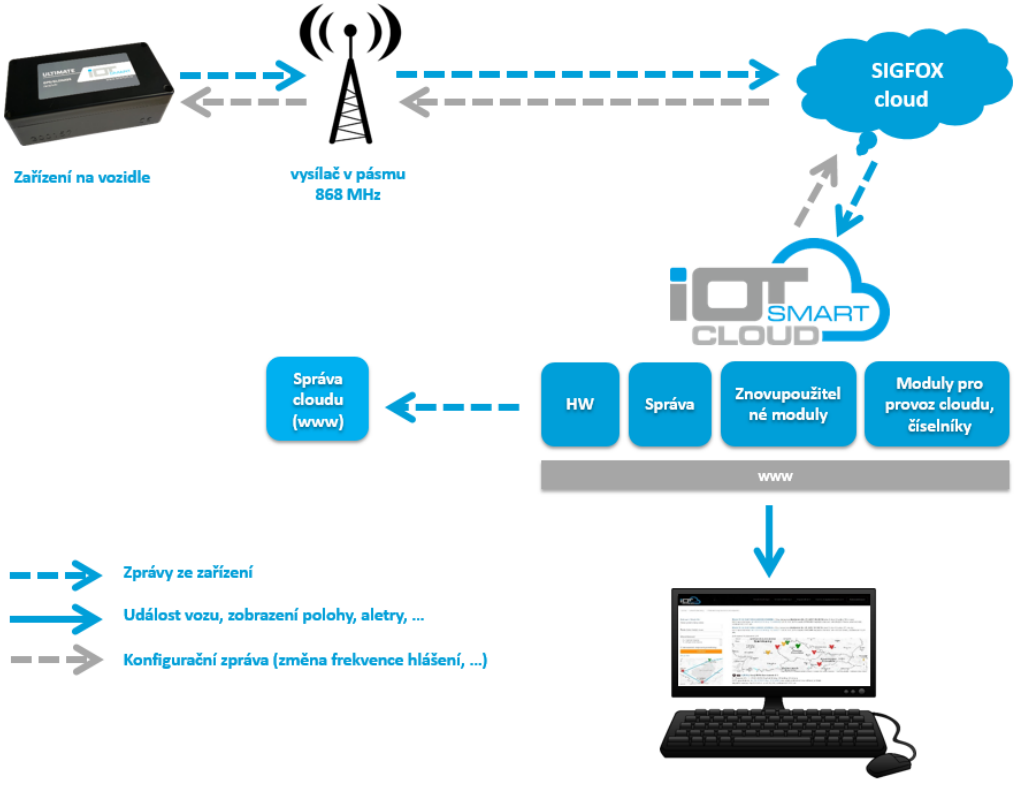
Internet věcí v oblasti domácností se dnes již běžně používá pod názvem smart home [46]. Nejde jen o pohodlí člověka, který si takovýto systém nechá nainstalovat. Jde také o dlouhodobou úsporu za výdaje spojené s vodou, elektřinou a i případně plynu. Dále IoT v prostředí chytrých domácností umožňuje výdaje za energie přehledně monitorovat [47]. Dále lze díky IoT zvýšit bezpečnost celého domu či bytu. Například lze nainstalovat chytré zámky do dveří. Tyto chytré zámky je snadné na dálku zkontrolovat jejich uzamčení nebo v případě nutnosti na dálku otevřít. Smart home je velmi obsáhlé téma a je zde spousta dalších zařízení, které mohou zlepšovat pohodlí, komfort ale i ochraňovat naše

zdraví, předcházet požárům a jiným haváriím. Například se může jednat o detektory kouře a plynu, senzory vlhkosti vzduchu, chytré termostaty kontrolující a regulující teplotu v domě atd. Velkým benefitem je pak možnost ovládání většiny zařízení v chytré domácnosti skrze chytrý telefon.

1.5.2 Doprava

V logistice jsou IoT systémy využívány například ke sledování stavu a umístění přepravovaného předmětu v reálném čase [48]. V této oblasti je hojně využívána technologie, což je družicový polohový systém, díky kterému je možné určit polohu ssledovaného zařízení.GPS [49].

Podobnou službu nabízí společnost IoT smart s.r.o. Jmenuje se Smart tracking a přenáší data pomocí sítě SIGFOX [50]. Dává uživateli informace o umístění přepravovaného předmětu, kterou si může zobrazit v mapě. Dále informuje o nárazech a může také monitorovat teplotu.



Obr. 4 Blokové schéma služby Smart tracking

Převzato z: [50]

1.5.3 Zemědělství

I v tomto odvětví dochází díky internetu věcí k velikým změnám a velkému pokroku vpřed. Cílem je zemědělství co nejvíce automatizovat a zefektivnit na základě informací poskytnutých z tzv. Smart farminig IoT zařízení.
To zahrnuje dálková ovládání automatických přístrojů a robotů na bázi GPS [51], kteří mohou provádět činnosti, jako pletení, postřikování, snímání vlhkosti, strašení ptáků a škůdců atd.. Takové systémy obstarávají automatické inteligentní zavlažování, které se řídí podle aktuálního počasí.

Další oblast kde nachází IoT uplatnění v rámci zemědělství je skladování úrody. IoT zde pomáhá například hlídat správnou teplotu, vlhkost, a také lze IoT využít k zabezpečení úrody proti krádeži.

IoT v zemědělství umožňuje zefektivnit veškeré pěstování rostlin i obilovin a pro farmáře to znamená větší výnosy s menšími ztrátami.

1.5.4 Lékařství

Péče o nemocného člověka vyžaduje dostatek pozornosti a stálý přísun informací o jeho aktuálním stavu. Při dnešních možnostech v oblasti senzorů můžeme sledovat velkou část činností našeho těla, což velmi usnadňuje práci doktorům a lidem pracujícím ve zdravotnictví. Například snímač EKG [52], který přenáší data do programu, který rozpoznává a analyzuje srdeční funkci. Dále měřiče krevního tlaku [53], teploty těla, zda má člověk dostatek kyslíku atd. Takové systémy ale mohou pomáhat i mimo nemocnice, kde můžou například hlídat životní funkce u starších osob, starat se o pravidelné a včasné braní léků a v případě nouze přivolat pomoc.

1.5.5 Energetika

V tomto odvětví se internet věcí využívá především k monitorování přenosových sítí.

To může poskytovat lepší přehled výrobcům, distributorům i koncovým uživatelům. Není možné přestavět sítě, které již dnes pracují, ale pomocí IoT je možné zlepšit kvalitu přenosu.

Například v jednotlivých budovách mohou senzory snížit výdaje za topení a osvětlení..

Zero – net buildings (ZNE) jsou budovy s nulovou spotřebou energie. Množství energie,

které se v celé budově spotřebuje, v horizontu let je rovno energii, která si budova s pomocí obnovitelných zdrojů vyrobí. Jedná se o systémy IoT, které kombinují solární panely, větrné turbíny, tepelná čerpadla a další zdroje elektrické energie k pokrytí spotřebované energie. [54]

Pojem IoT technologie v energetickém sektoru je ale mnohem rozsáhlejší téma, týkající se hlavně inteligentních energetických sítí. Některé společnosti již začínají tyto sítě využívat. Jejich hlavní výhodou je naprostý přehled o aktuální spotřebě energie.

1.5.6 Smart City

Růst populace a zvýšená urbanizace vyvolávají ve městech řadů problémů ať už sociálních, organizačních, ekologických, nebo ekonomických. Rychlý růst města například způsobuje dopravní zácpy, velké znečištění a také sociální nerovnost. V této souvislosti začala vznikat otázka, jak tyto problémy řešit a zajistit tak budoucí životaschopnost a prosperitu v metropolitních oblastech. Jako dobré řešení se nabízí využití vyspělých technologií a vybudování tak zvaných chytrých měst (Smart City). [55]

Hlavní myšlenkou Smart city je využít obrovské množství dat získaných z IoT zařízení k lepšímu plánování a řízení každodenních činností ve městě. Nejprve ale musí město fungovat jako komplexní síť vzájemně propojených systémů, která zprostředkovává nová data, která se využijí k lepšímu rozhodování, předcházení a řešení problémů, a také k zefektivnění mnoha činností [56].

Ze studie [57] můžeme odpozorovat, že koncept Smart city kombinuje aplikace IoT uvedené výše v této práci. Ta definuje hlavní aspekty chytrého města jako komplexní síť všech uvedených odvětví.

Obr. 5 Ukázka Smart City

Převzato z: [57]

Existuje mnoho definicí chytrého města a každá společnost zabývající se touto problematikou prezentuje svojí originální definici. Koncept Smart city se liší v závislosti na úrovni rozvoje konkrétního města, ochoty země, zdejších zdrojích atd. [58].

Například Britské ministerstvo pro podnikání a inovace (BIS) ho definuje spíše jako proces, kdy se angažovaní občané snaží zlepšit infrastrukturu města, sociální kapitál, životaschopnost atd. pomocí digitálních technologií. Společnost IBM pojem Smart city definuje jako město, které optimálně využívá všech spolupracujících technologií, které jsou v současnosti dostupné, k lepšímu řízení procesů a optimalizaci využití omezených zdrojů [59].

2 Bezpečnost

2.1 Proč je nutné zabezpečovat IoT

Bezpečnost dat je u této problematiky rozhodně jedním z největších problémů, který je nutno řešit. Vzhledem k velkému množství přenášených informací rámci IoT aplikací by měl být systém dostatečně chráněn. Podle [60] je největším problémem dostupnost, integrita a zabezpečení dat.

Dále musíme uvažovat rozmanitost používaných zařízení a množství komunikačních protokolů. Možné hrozby se mohou vyskytovat ve všech vrstvách systému. Zabezpečení by tedy mělo být obsaženo také ve všech uvedených vrstvách [61].

Hrozbou může být například nedostatečné šifrování při přenosu dat, nedostatečná autentizace, nebo neověřená síťová služba. V síťové vrstvě je tedy bezpečnější volit ověřené sítě. Také nesprávná webová a cloudová rozhraní mohou být zranitelná místa. To může vést k útoku na úrovní aplikační vrstvy. Zde se k odstranění hrozeb může využívat biometrie a víceúrovňová autentizace [62]. Hlavním cílem je zachování soukromí, bezpečnost dat, ale i bezpečnost využívaných zařízení.

2.2 Možné problémy

[63]

Kvalita shromažďovaných dat je kritická pro správnou funkci chytrých zařízení a systémů, ať už jde o domácí, průmyslové, nebo jiné aplikace internetu věcí. Dalším problémem je správnost dat. Správnost může být ovlivněna mnoha faktory jako například: lidská chyba, opotřebení zařízení, nebo útoky hackerů. Podle některých studií může například nadbytek elektrického šumu v bezdrátových sítích vést ke špatné funkci, nebo dokonce selhání systému. Mnoho podnikových i průmyslových infrastruktur mají značné bezpečnostní mezery, které mohou využívat útočníci k napadení daných systémů. Například výbuch v ropné rafinérii v Texasu zabil patnáct lidí a dalších 180 zranil. Příčina je z části přisuzována zařízením, která poskytovala nesprávné data. Velké tragédie mohou také nastat ve spojitosti s chytrými zdravotnickými potřebami.

Příčinou nesprávných dat mohou být tedy opotřebené, nebo špatně fungující senzory, ale také lidská chyba. Například se senzory mohou jevit jako nefunkční, ale jejich data mohou být pouze zkresleny. Například pokud zakryjeme teplotní senzor, podle kterého se řídí klimatizace v místnosti, nebude poskytovat správná data i přes to, že je naprosto v pořádku. Podle některých studií je lidská chyba nejčastější příčinou chybných dat.

Dalším velmi častým problémem jsou útoky hackerů, kteří nejčastěji využívají zranitelností zařízení a senzorů. Zranitelnost koncových zařízení (senzor) je velmi běžná jelikož vývojový inženýři, kteří konstruují takováto zařízení, nejsou odborníci na kybernetickou bezpečnost. Důsledky nekvalitních dat, nebo hackerských útoků se mohou značně lišit podle aplikace dané infrastruktury. Například diametrálně odlišné škody nastanou při poruše běžného „IoT“ zařízení, při útoku na chytrou domácnost anebo při útoku na nějakou průmyslovou IoT aplikaci/infrastrukturu. V oblasti průmyslu například každá minuta kdy stojí výrobní linka je pro danou společnost ztráta.

2.3 Reálné útoky

Jeep Hack

[64]

V tomto případě se jednalo pouze o demonstraci, čeho všeho by útočníci mohli dosáhnout při používání vozidel využívající chytré asistenty společně s internetovým připojením, bez dostatečného zabezpečení.

Nejprve se dvojice vědců pokusila proniknout do multimediálního systému Jeep prostřednictvím lokální Wi-Fi, kterou byly některé modely vybaveny. Hesla k Wi-Fi jednotlivých vozů byly generovány automaticky v závislosti na datu a času, kdy bylo vozidlo poprvé uvedeno do provozu. Pokud je tedy znám rok, případně měsíc uvedení vozidla do provozu, je možné heslo odhalit během jedné hodiny. Nevýhodou je, že po celou hodinu musí být útočník ve spojení s Wi-Fi napadeného vozu. Přesným stanovením času a datem výroby byli ale schopni snížit počet možných kombinací a heslo získat během pár minut.

Po připojení k řídící jednotce automobilu dokázali využít softwarových nedostatků a převzali kontrolu nad systémem řídící jednotky. Byli tak schopni ovládat hudební přehrávač, topení, nebo sledovat polohu vozidla pomocí GPS. Takto napadli auto, které mělo ve výbavě vestavěnou lokální Wi-Fi, ale v té době tuto možnost využívalo jen pár zákazníků. Hledali tedy jiné možnosti, jak napadnout vozidla bez tohoto prvku. Přišli na to, že všechny řídící jednotky vozů Chrysler jsou připojeny na celulární síť Spirit a pokusili se tohoto faktu využít. Pomocí femtocellu (mobilní základová stanice) se dokázali dostat do sítě Spirit a spravovat hromadné skenování IP adres. Takto mohli nabourat všechny modely vybavené stejným typem řídící jednotky.

Dalším krokem bylo získat přístup k sběrnici CAN (Controller area network), která slouží jako interní síť vozidla a přes kterou jsou elektronicky ovládány všechny důležité komponenty vozidla. Aktualizovali tedy řídící jednotku a nahráli jimi vytvořený kód, který umožnil přístup i do sběrnice CAN. Po tomto kroku měli nad vozem již naprostou kontrolu. Pomocí parkovacích asistentů, které jsou schopné pohybovat volantem, mohli auto řídit a skrze elektronický plyn mohli vozidlo zrychlovat. U takovýchto vozidel je

elektronicky řízená většina prvků ovlivňující jízdu a celé vozidlo obsahující chytré systémy funguje jako systém internetu věcí.

Tato demonstrace vystihuje nutnost, z jakého důvodu musí být IoT maximálně zabezpečeno. V případě, že dojde k poškození zařízení, dochází samozřejmě k nějaké „finanční škodě“ je to hrozné ale v nejhorším scénáři může „někdo“ přijít o to nejdůležitější – o život. A proto je nutné dbát na zabezpečení internetu věcí, ať se jedná o jakoukoliv věc senzor nebo „chytré auto“

Botnet IoT

Botnet v případě internetu věcí představuje skupinu spolupracujících zařízení, které jsou napadené škodlivým kódem a jsou pod kontrolou útočníka. IoT botnet může být navržený tak, aby prováděl nechtěné a škodlivé úkony, jako zasílání spamu, krádež dat, nebo plánované a koordinované útoky typu DDoS cílených proti celým infrastrukturám [65].

Mirai botnet

[66]

Nejznámějším malwarem spojovaným s IoT botnetem je nejspíše kód zvaný Mirai. Ten stojí za velkým DDoS útokem v roce 2016 na společnost Dyn, která poskytuje DNS pro služby, jako Twitter, Spotify, GiftHub, Reddit atd.. To způsobilo několikahodinový výpadek těchto služeb.

Jde o útok, který pomocí malwaru mirai infikuje počítače, ty následně scanují IP adresy a hledají IoT zařízení. Jde především o domácí modemy, routery, kamery s vlastní IP adresou a další IoT zařízení. Následně u nich zkouší využít všeobecně známé zranitelnosti. Při úspěšném provedení útoku vzniká velké množství IoT zařízení, které jsou ovládány útočníkem.

Csino hack

[67]

V roce 2018 došlo ke kybernetickému útoku na nejmenované casino v Americe. Útočníci využili nezabezpečený chytrý teploměr, který snímal teplotu vodu v akváriu. Přes něj pronikli do sítě casina a získali přístup k databázi registrovaných hráčů.

2.4 Jak zabezpečit jednotlivé vrstvy

2.4.1 Senzorická vrstva

Tato vrstva má za úkol sběr fyzických dat. Jsou v ní obsaženy různé typy sběrných modulů, jako mohou být snímače teploty, vlhkosti, zvuku, vibrací, tlaku atd. Dále tuto vrstvu můžeme rozdělit na percepční zařízení a percepční síť [68]. Senzorické zařízení slouží pro samotný sběr dat a jejich řízení, kdežto senzorická síť získané data odesílá do brány, nebo do řídící jednotky.

Možnost, jak tuto vrstvu zabezpečit je například detekce abnormálních jevů přímo na senzorovém zařízení. Jako abnormální jev se považuje fyzické napadení snímače (poškození, nebo úplné zničení) i kybernetický útok. Při detekci takového jevu je snímací zařízení považováno za vadné. IoT systém musí takové zařízení rozpoznat a následně provést opatření, aby systém nebyl na základě tohoto vadného uzlu dále ovlivněn a ohrožen.

Další variantou jak tuto vrstvu napadnout je použití kryptografických algoritmů a prolomení mechanismu klíčování.

Pro zachování soukromí při odesílání citlivých dat na sběrný server je důležité anonymizovat data, aby se sběrný server nemohl vrátit zpět k odesílanému zařízení. Možnost, jak data anonymizovat se uvádí například v práci [69]. Jedná se o anonymní protokol, který se skládá ze dvou fází. První fáze má za úkol rezervaci místa pro odesílanou informaci. To provádí pomocí skupiny určitého počtu uživatelů, kteří si navzájem přiřadí slot na přijímací části pro zprávu, která má být odeslána. Jednotliví uživatelé se navzájem neovlivňují a neinterferují ani se sběrným serverem. Druhou fází je přenesení kódovaných dat na sběrný server. Ten ale nemůže spojit přijaté informace s konkrétním IoT zařízeníma následně je přerušeno spojení, takže je zajištěna bezpečnost informací, která jsou tímto způsobem zpracovávána.

Takovéto zabezpečení je důležité například při použití IMD (Implantable medical devices – implantované zdravotní zařízení), které je implantováno do lidského těla. Má za úkol diagnostikovat, monitorovat, ale také může zajišťovat určité terapeutické činnosti. Zde je obzvláště důležité zabezpečení a je vhodné používat pro komunikaci takovýchto zařízení anonymizovaný protokol, protože úspěšně vedený útok může znamenat ohrožení života pacienta.

Je potřeba také uvažovat možnost útoku fyzického charakteru na systémy IoT. Prvním stupněm ochrany před útokem na jakékoliv fyzické zařízení IoT by tedy mělo být zabránění fyzickému kontaktu nežádoucím osobám. Například do budovy, ve které je instalovaný IoT systém, který chceme ochránit. K IoT systému by tedy měli mít přístup pouze pověřené osoby. Kontrola pověření osoby může probíhat pomocí přístupových karet, zadávání hesel či skrze biometrické zabezpečení (čtení otisků prst, rozpoznávání obličeje, rozpoznání duhovky).

Pokročilejším zabezpečením je zabránění útoku při manipulaci s určitým zařízením. Napadením hardwaru se zabývá [70] a [71], které uvádí útoky využívající implementaci chyby do zařízení (Fault attack) a postranní kanály (Side channels). Pomocí takovýchto útoků je možné analyzovat data z napadených zařízení a tím získat tajné klíče využívané například k šifrování přenášených dat nebo k ověřování aktualizací firmwaru prováděných bezdrátově tzv. OTA aktualizace (over the air).

2.4.1.1 Side attacks

[72]

Útok postranním kanálem, neboli side channel attack je útok, při kterém se využívá úniku informací z fyzické implementace systému, které jsou jakkoliv závislé na tajném klíči algoritmu. Podle [bělohoubek] dělíme tyto útoky na: Neiivazivní útoky, do kterých patří časová a odběrová analýza (Sipmle Power Analysis - SPA), diferenční odběrová analýza (Differential Power Analysis - DPA) a analýza EM vyzařování. Dále poloinvazivní útoky, kde jde o injekci přechodových poruch, například EM impulzem, nebo laserovým paprskem. Poslední jsou invazivní útoky, které jsou prováděny injekcí trvalých poruch.

Nejpoužívanějším typem útoku postranním kanálem je **Power analysis** (výkonová analýza), která využívá informace o spotřebě energie. Analýza spotřeby energie pracujícího kryptografického zařízení může útočníkovi poskytnout informace

o provedených operacích a citlivých kryptografických výpočtech.

Při SPA mohou být utajované informace získány z jednoho, nebo více měření spotřeby energie. V DPA se tvoří statistika pomocí měření velkého množství dat o spotřebě, aby se zjistily rozdíly mezi různými výpočty. Tyto rozdíly se následně využívají ke zjištění správného klíče.

Další možností je měření elektromagnetické energie (EM) kterou zařízení vyzařuje. Výhoda je, že tato metoda lze provádět bezdrátově, nevýhody jsou obtížnost zpracování naměřených hodnot a nízký poměr signál/šum.

Jako ochrana proti útokům postranními kanály se zavádí do kryptografických výpočtů určitá náhodnost s použitím speciální logiky, která má datově nezávislou spotřebu energie.

2.4.1.2 Fault attacks

[70]

Existuje více způsobů, jak do zařízení implementovat chybu. Odlišné chování napadeného zařízení (chyba) způsobuje abnormální funkci tranzistorů. Všechny způsoby mají jednu společnou vlastnost, a to manipulaci se zařízením ve fyzické vrstvě. Naopak se liší v charakteru chyb, které jednotlivé útoky způsobují.

Prvním útokem je **Under-Powering and Power Spikes**, což v překladu znamená podpěťové a napájecí špičky. Možnost, jak v zařízení vyvolat chybné chování je nedostatečné napájení zařízení. U této metody ale nelze výkyvy napájení načasovat a je pro útočníka složité zpracovat informace poskytnuté napadeným zařízením. Dalším způsobem, jak ovlivnit výpočty prováděné v napadeném zařízení jsou pravidelné výkyvy napájecího zdroje na vyšší hodnotu. Takovéto výkonové špičky mohou způsobit poruchy paměti a chybnou funkci procesoru.

Clock Glitches je metoda, kdy je na zařízení přivedený jiný průběh napájecí energie. Jedná se o jeden, nebo více kratších impulzů, než jsou obvykle přiváděny na zařízení. To způsobuje, že procesor začne provádět další akci ještě dříve, než dokončí předchozí. Tento útok se provádí nejčastěji na čipové karty.

Temperature attacks (tepelné útoky) je typ útoku, který využívá změnu teploty, aby zařízení přestalo správně pracovat. Využívá se ke změně dat uložených v paměti.

Optical attacks, neboli optické útoky jsou prováděny na odkrytý čip pomocí fotografického blesku, nebo laserového paprsku. To způsobuje přepnutí tranzistoru. Je tedy možné například pomocí soustředěného laserového útoku nastavit, nebo resetovat jeden bit v paměti a vyvolat tak poruchu.

Electromagnetic fault injection, extérní elektromagnetické pole způsobuje poruchu zapouzdřeného čipu, nebo změnu obsahu paměti. Tuto chybu je možné vyvolat i pomocí běžného plynového zapalovače, ale takové elektromagnetické pole se nedá přesně kontrolovat.

Proti těmto útokům neexistuje žádné opatření, které by zařízení ochránilo před všemi typy. Pro dostatečné zabezpečení je zapotřebí kombinace více bezpečnostních technik. V praxi ale nelze zařízení zabezpečit natolik, aby bylo nenapadnutelné. Vždy se volí taková opatření, aby byl útok co nejsložitější a nejdražší.

Jsou známy dva hlavní principy ochrany zařízení před těmito útoky. Prvním způsob je hardwarová ochrana. Tu dále dělíme na aktivní a pasivní. Pasivní ochrana je kupříkladu kovová vrstva, která chrání čip před optickými útoky. Aktivní ochranou se myslí aktivní stínění (drátěným pletivem), kterým prochází signály a detekují jakékoliv přerušení stínící vrstvy. Dále mohou být čipy chráněny světelnými senzory a detektory abnormálních frekvencí. Hlavní nevýhodou těchto opatření jsou hlavně vysoké náklady.Druhým principem je ochrana kryptografického algoritmu a případná detekce injektované chyby. Toho lze dosáhnout například pravidelnou kontrolou, zda bylo s výpočtem v procesoru manipulováno. Kontrola může probíhat pomocí redundance. To znamená, že když se objeví redundantní data, značí to narušení výpočtu. Další možností je navrhnutí implementace tak, aby byla ze své podstaty náchylnější k útoku, a tím dochází ke snadnější kontrole.

2.4.2 Transportní vrstva

V internetu věcí jsou zařízení mezi sebou propojovány prostřednictvím různých technologií. Může jít například o spojení heterogenních sítí, jako jsou WSN, mobilní sítě, RFID systémy a WLAN. Zajištění komunikace mezi zařízeními je nezbytné pro spolehlivou výměnu informací. To vyžaduje bezpečné, spolehlivé a škálovatelné připojení internetu věcí. Pro internet věcí je tedy výhodné používat již stávající komunikační protokoly, jako je IPv6. Mezi základní principy bezpečné komunikace v internetu věcí patří autentizace, dostupnost, důvěrnost a integrita. Komunikační systémy by tedy měly být

navrženy tak, aby byly dostatečně zabezpečené. To znamená najít takovou hranici, která je ekonomicky přípustná a zároveň poskytuje zabezpečení dostatečné na to, aby bylo potřeba při pokusu o napadení vynaložit příliš velké úsilí, což nutí útočníka ke vzdání útoku. Běžně používané komunikační protokoly a potenciální bezpečnostní funkce zahrnují:

- RFID (např. ISO 18000 6c EPC tř. 1 gen. 2), bezpečnostní funkce zahrnují důvěrnost, integritu a dostupnost
-)
- NFC, IEEE 802.11 (WLAN), IEEE 802.15.4, IEEE 802.15.1 (Bluetooth), v těchto bezdrátových komunikačních technologiích je pro zabezpečení potřeba: důvěrnost, integrita, autentizace, dostupnost a detekce škodlivého vniknutí.
- IETF 6LoWPAN. Vzhledem k tomu, že 6LoWPAN je kombinace IEEE 802.15.4 a IPv6, musíme uvažovat možné potenciální slabá místa z obou stran.
- Machine-to-Machine (M2M), musíme uvažovat nejčastější útoky typu DoS při spojení M2M
- Tradiční IP technologie, jako je IPv6 a IPsec můžeme zajistit autentizaci a integritu pomocí „autentizační hlavičky“ a určité zapouzdření zařízení poskytuje důvěrnost. V poslední době se využívá zabezpečení přenosové vrstvy vzájemnou autentizací dvou stran pomocí veřejných klíčových infrastruktur a X.509 certifikátů.
- Správa klíčů v internetu věcí. V poslední době bylo navrženo mnoho klíčovacích systémů, jako například KMS, který by měl být navržen na základě standartních protokolů. IP sec používá IKE – Internet Key Exchange pro automatickou správu klíčů. Pro 6LoWPAN IPsec a IEEE 802.15.4 je navržena správa klíčů IKEv2

2.4.2.1 Kabelová komunikace

Největší rozdíl mezi bezdrátovou a kabelovou sítí v oblasti bezpečnosti je ten, že kabelové sítě lze napadnout, pouze když dojde k fyzickému kontaktu s nějakou částí sítě. Z toho můžeme usuzovat, že obecně jsou kabelové sítě bezpečnější. Nevýhodou kabelových sítí však zůstává nutnost fyzického propojení, což omezuje pohyb připojeného zařízení.

2.4.2.2 WLAN

Wi-Fi

Získání přístupu k domácí síti Wi-Fi umožňuje útočníkovi provádět útoky na jakékoli připojené zařízení. Pro přístup do celé sítě stačí znát přístupové heslo, což je obecně velmi malý stupeň zabezpečení. Standard Wi-Fi Wired Equivalent Privacy (WEP)

je považován za ne příliš zabezpečený a neměl by být používán. Ačkoli novější technologie Wi-Fi Protected Access II (WPA2), využívající šifrování, je více zabezpečená, útočníci stále mohou útočit na síť pomocí Dictionary attack (opakovaná snaha o uhádnutí přístupového hesla) a snažit se získat přístup k síti [73]. Při takovémto útoku pak nejvíce záleží na složitosti hesla.

V roce 2018 společnost WiFi Alliance oznámila vydání nového standardu WPA3, který by měl postupně nahradit WPA2. Ale ani tato technologie se neprokázala, jako příliš bezpečná a již bylo odhaleno několik slabých míst [74].

Všechny moderní mechanismy zabezpečení WiFi používají dvě hlavní techniky: autentizační protokoly, které identifikují zařízení, snažící se připojit k síti; a šifrování, které zajistí, že pokud útočník „odposlouchává“ zasílaná data, nebude mít přístup k důležitým datům.

Z-Wave [75], [76]

Hlavním bezpečnostní prvkem používaným v této síti je AES 128 šifrování pro přenos informací v této síti. Když se do této sítě poprvé připojuje nové zařízení, musí být vybaveno štítkem obsahující QR kód, nebo PIN kód, kterým se nevé zařízení musí autentizovat. Dále se zde využívá bezpečná výměna klíčů Elliptic Curve Diffie-Hellman (ECDH) a pokud uživatel společně s touto sítí využívá cloudové služby, Z-Wave využívá protokol TLS 1.1 pro komunikaci s cloudem.

ZigBee [77]

Zabezpečení je zde realizováno podle modelu IEE 802.15.4, který obsahuje mechanismy, jako je řízení přístupu (autentizace), šifrování a integritu. Ta je pravidelně kontrolována (MIC).

Celá architektura zabezpečení je založena hlavně na šifrování a má propracovaný protokol správy klíčů. Používají se zde 3 různé typy klíčů pro připojení k síti, skupině zařízení, nebo propojení dvou zařízení. Prvním typem je hlavní klíč (Master key), ze kt kterého jsou vytvořeny propojovací klíče. Vzhledem k jeho důležitosti musí být počáteční hlavní klíč získán bezpečnými prostředky (předinstalace nebo přenos klíče - vysvětleno níže). Další typ se nazývá Odkazový klíč (Link key) a šifruje komunikaci point-to-point na aplikační úrovni. Je znám pouze u prvků, které se tohoto odkazu účastní. Tento klíč je

sdílen pouze mezi dvěma síťovými prvky a je odlišný pro každou dvojici prvků. Odkazový klíč se používá k minimalizaci bezpečnostních rizik souvisejících s distribucí hlavního klíče. Poslední je Síťový klíč, který se používá na úrovni přenosu a je známý všemi prvky, které k němu patří. Síťový klíč se používá ve skupinách více než dvou prvků v síti.

Pro zajištění bezpečnosti je důležité správné připojení. První metou je předinstalace (preinstallation), která je důležitá pro hlavní klíč. Výrobce určitého zařízení do něj zabuduje hlavní klíč – předinstaluje je do zařízení. Uživatel následně využije hlavní předinstalovaný klíč k připojení.

Další metodou je přemístění klíčů (key transport). Zařízení pošle do sítě – konkrétně do centra zabezpečení, kde se ověřuje validita požadavku, požadavek na zaslání klíče. Tato metoda je platná pro vyžádání kteréhokoli ze tří typů klíčů. Centrum zabezpečení může fungovat dvěma způsoby.

Komerční režim (commercional mode): Centrum zabezpečení samo o sobě vede seznam zařízení, hlavních klíčů, propojovacích klíčů a síťových klíčů. V tomto režimu vzroste paměť vyžadovaná střediskem důvěry v závislosti na počtu zařízení přidružených k síti.

Soukromý režim (residential mode): Centrum zabezpečení uchovává pouze síťový klíč a řídí přístup k síti, ostatní informace jsou uloženy v každém uzlu. Paměť, kterou vyžaduje Centrum zabezpečení, nezávisí na velikosti sítě. V tomto případě nelze ověřit, zda byla pořadová čísla modifikována třetí stranou.

Poslední metoda připojení je vytvoření klíče bez komunikace (Key establishment without communication). Toto je metoda generování odkazových klíčů na základě hlavního klíče pro dvě zařízení, aniž by bylo nutné komunikovat. Tato služba ZigBee je založena na protokolu SKKE (Symmetric-Key Key Establishment) . Zařízení zapojená do komunikace musí vlastnit hlavní klíč, který mohl být získán předinstalováním nebo přenosem klíčů.

Hlavní slabost v implementaci bezpečnostních mechanismů Zigbee je přímo odvozena z omezených zdrojů zařízení protože většina z nich je napájena z baterií, proto mají malý výpočetní výkon a paměť. Klíče používané v zařízeních ZigBee jsou uloženy v paměti, což znamená, že útočník může jednoduše přečíst klíč přímo z paměti (se specializovaným softwarem), pokud má k zařízení fyzický přístup. Použitím mikrokontroléru, který zajistí bezpečnou autentizaci, je možné předejít tomuto riziku.

2.4.2.3 LPWAN

Jde o sítě s velkým dosahem, malou energetickou náročností a poměrně levným provozem. V České Republice se v této kategorii nejvíce využívají SIGFOX, LoRaWan a NB-IoT, jejichž zabezpečení je popsáno níže.

sigfox [78]

Sigfox používá mezi připojenými zařízeními end-to-end autentizaci založenou na tajných klíčích mezi připojenými zařízeními a jejím cloudem. Tento tajný klíč je uložen v nepřístupné paměti spojené s viditelným a specifickým ID uloženým v paměti jen pro čtení. Tajný klíč se používá ve zprávách odeslaných zařízeními k vytvoření podpisu, který je jedinečný pro každou zprávu a který ověřuje odesilatele. Tento podpis obsahuje pořadové číslo, aby nedocházelo k nechtěnému opakování zasílání zpráv. Každá zpráva je zasílána třikrát a pokaždé na jiné náhodné frekvenci, to podporuje zabezpečení proti úniku tajných dat. Na úrovni připojených zařízení se využívá proces downlink SIGFOX, což je zasílání zpráv od uživatele k zařízení. Komunikace probíhá nauživatelemzvolené frekvenci a pouze určitý počet zpráv. To zamezuje přijímání zpráv od hackerů. Základové stanice jsou spojeny s cloudem point-to-point pomocí virtuální privátní sítě (VPN) a data jsou šifrovány. Také samotný cloud pracuje na privátních serverech, které jsou poskytovány zabezpečenými datovými centry. IT platformy zákazníků také připojené ke cloudu jsou chráněny pomocí rozhraní šifrovaných HTTPS pro web a zpětnou komunikaci.

LoRaWan[79]

Tyto sítě používají dvě bezpečnostní vrstvy – jednu vrstvu pro síť, druhou pro aplikace. Síťovou bezpečnost zajišťuje autentizace koncového zařízení k jednotlivému síťovému uzlu. Na straně aplikační vrstvy se zajišťuje bezpečnost tím, že síťový operátor nemá přístup k aplikačním datům uživatele. Aplikační data koncového uživatele jsou navíc zakódována pomocí AES metody používající k výměně klíče IEEE EUI64 identifikátor.

Než může zařízení spolupracovat se sítí LoRaWan, musí být aktivováno. To je možné provést dvěma způsoby OTAA (Over-The-Air Activation) a APB (Activation By Personalisation).

OTAA je zkratka pro bezdrátovou aktivaci, která je založena na bezdrátové komunikaci zařízení se sítí. Každému uzlu (koncovému zařízení) je přiřazen 64bitový DevEUI, 64bitový AppEUI a 128bitový AppKey. Dev EUI je globálně jedinečný identifikátor zařízení, které ma 64bitovou adresu srovnatelnou s MAC adresou pro zařízení TCP/IP. AppKey se používá pro kryptografické podepsání požadavku na připojení. Všechny tyto faktory jsou zpřístupněny aplikačnímu serveru, ke kterému se chce zařízení připojit. AppKey se používá, když koncové zařízení odešle zprávu s požadavkem na spojení. Zařízení odešle zprávu s požadavkem na spojení složenou z jeho AppEUI a DevEUI. Navíc odešle DevNonce, což je jedinečná, náhodně generovaná dvoubajtová hodnota použitá pro zabránění útoků opakovaným zasíláním požadavků na spojení. Pokud server přijme požadavek na spojení, aplikační a síťové servery vypočítají dva 128bitové klíče uzlu (AppSKey) a (NwkSKey). Vypočítávají se na základě hodnot odeslaných ve zprávě Žádost o spojení z uzlu. Aplikační server navíc vygeneruje svou vlastní nenulovou hodnotu AppNonce. To je další jedinečná, náhodně generovaná hodnota. Následně server odešle do zařízení zprávu obsahující AppNonce, NetID a adresu koncového zařízení (DevAddr) spolu s kanály, které mají být použity (CFList). Adresu zařízení je možné použít k rozlišení mezi koncovými zařízeními, která se již připojily k síti. To umožňuje síťovým a aplikačním serverům používat správné šifrovací klíče a správně interpretovat data. Při zpětném příjmu dat jsou data šifrována pomocí AppKey. Uzel poté pomocí AppKey dešifruje data a odvozuje AppSKey a NwkSKey pomocí hodnoty AppNonce obdržené v odpovědi Připojit přijmout.

Další možností je aktivace personalizací (ABP). Tato metoda se liší od OTAA, tím, že jsou koncová zařízení dodávány s DevAddr a oběma klíči relace (NwkSKey a AppSKey), které jsou pro zařízení jedinečné. Protože zařízení již mají potřebné informace a klíče, mohou začít komunikovat se síťovým serverem bez potřeby výměny zpráv o připojení. Koncové zařízení se připojuje k síti LoRaWAN prostřednictvím požadavku OTAA nebo ABP, po připojení jsou všechny budoucí zprávy šifrovány a podepsány pomocí kombinace specifických klíčů

NB-IoT [80]

V těchto sítích se využívá šifrování dat, což zajišťuje jejich bezpečný přenos. NB-IoT používá protokol UDP, který je poměrně jednoduchý a jeho hlavní výhodou je nízká energetická spotřeba. Tento protokol totiž pro přenos dat nepotřebuje navázat spojení se zařízením, do kterého, data zasílá. Nevýhodou je, že při přenosu dat za použití tohoto protokolu jsou data při cestě internetem viditelná třetím stranám. To je ze své podstaty nebezpečné a musíme proto do takovéto sítě přidat určité prvky zvyšující bezpečnost dat.

První možností je APN (Access Point Name), což je možnost, kterou nabízí někteří operátoři, a jde o použití přechodného serveru, který shromažďuje data ze sítě, aniž by data procházela internetem. Konečná zákazníkova platforma je připojena přes zabezpečenou VPN (Virtual Private Network) k platformě operátora, čímž je zabezpečena celá komunikace. Výhodou tohoto typu zabezpečení sítě je rychlý vývoj a úroveň zabezpečení, naopak nevýhodou jsou vyšší náklady pro zákazníka a malá flexibilita při změně operátora.

Druhou mozností je zabezpečení samotného protokolu UDP, kdy se využívá šifrování end-to-end společně s autentizací, za kterou je zodpovědný cloud poskytovaný operátorem. Výhodou je vysoká úroveň zabezpečení nezávisle na provozovateli sítě.

2.4.2.4 Šifrování dat

[81]

Hlavním účelem šifrování je udržovat citlivá a důvěrná data v anonymitě před nežádoucími uživateli, kteří by mohli data jakkoliv zneužít. Zjednodušeně lze říci, že šifrování je proces, kdy probíhá kódování dat do nečitelného formátu pomocí speciálního šifrovacího klíče. Zpětně je pak možné data dešifrovat pouze pomocí speciálního tajného dešifrovacího klíče. Tento typ ochrany údajů je zatím patrně nejlepším dostupným. Bez šifrování je jakákoli část dat nebo zprávy čitelná pro kohokoli, kdo je schopen zachytit data při přenosu, nebo ukrást data uložená na serverech.

Nejběžnější metody šifrování jsou podle [82] jsou:

- Data encryption standard (DES)

  Národní formalizační a technologický institut vlády USA (NIST) dohlíží na tuto formální šifrovací metodu. DES používá stejný šifrovací klíč k šifrování a dešifrování dat. Odesílatel i příjemce musí mít stejný tajný klíč. Důležitý rozdíl

mezi DES a AES je v tom, že DES je méně bezpečný než AES. DES je základním kamenem kryptografie, ale v současné době existují mnohem účinnější metody.

- TripleDES

  Tento algoritmus je typ počítačové kryptografie, kde každý blok dat přijímá tři průchody. Další zabezpečení pochází z větší délky klíče. Triple DES byl nahrazen AES. Triple DES je nyní považován za zastaralý, ale některé IoT produkty ho stále používají kvůli jeho kompatibilitě a flexibilitě. Triple DES zajišťuje ochranu před útoky hrubou silou. Útok hrubou silou je založený na opakování pokusů (na rozdíl od intelektuálních strategií) prolomit zabezpečení zařízení. Útoky hrubou silou používají automatické nástroje k hádání různých kombinací, dokud hacker nezíská tajný klíč.

- RSA

  Šifrování RSA využívá technologii šifrování veřejných klíčů licencovanou společností RSA Data Security, která také prodává své doprovodné vývojové sady. Šifrování RSA umožňuje uživatelům odesílat šifrované informace bez nutnosti předchozího sdílení kódu s příjemcem. Jedná se o šifrování veřejného klíče a veřejný klíč lze otevřeně sdílet. Data však lze dešifrovat pouze jiným soukromým klíčem. Každý uživatel RSA má společný veřejný klíč, ale soukromý klíč potřebný k dešifrování je určen pouze příjemcům.

- AES

  Advanced Encryption Standard používá jediný šifrovací klíč různých délek. Algoritmus AES se soustředí na jeden blok dat a překóduje je 10 až 14krát, v závislosti na délce klíče. AES je efektivní algoritmus, jehož síla spočívá v jeho klíčových možnostech délky. Čím větší je délka klíče, tím exponenciálně obtížnější je prolomit šifrování.

- Twofish

  Twofish používá systém šifrování založený na jediném klíči libovolné délky až 256 bitů. Tento šifrovací standard je účinný u počítačů s procesory s nízkou

výpočetní kapacitou, čipových karet a zařízení IoT. Twofish se objevuje v mnoha bezplatných šifrovacích softwarových produktech, jako je například VeraCrypt.

Neexistuje jedno konkrétní řešení pro ochranu všech systémů IoT, protože většina zařízení používá různé řídicí platformy, servery, domény připojení a protokoly. Data jsou ukládána na serverech a každý, kdo k nim má přístup, musí být ověřován, aby bylo zaručeno soukromí a exkluzivita dat. Proto by mělo být implementováno šifrování k ochraně a izolaci dat mezi uživateli, společnostmi a dalšími zúčastněnými osobami nebo s přístupem k datům. Šifrování by tedy mělo být jádrem každého zařízení IoT, aby se dosáhlo stavu, ve kterém jsou data plně šifrována při ukládání i přenosu.

2.4.3 Aplikační vrstva

Protože IoT stále nemá globální zásady a standardy, kterými by se řídili jednotlivé infrastruktury, existuje mnoho problémů souvisejících s bezpečností aplikací. Různé aplikace mají různé autentizační mechanismy, což činí jejich integraci velmi obtížnou, aby bylo zajištěno soukromí dat. Velké množství připojených zařízení, která sdílejí data, způsobují velké požadavky na aplikace, které data analyzují, což může mít velký dopad na dostupnost služeb. Dalším problémem, který je třeba vzít v úvahu při navrhování aplikací v IoT, je to, jak budou různí uživatelé s aplikacemi zacházet a jaké bude množství dat, která budou zpracovávána, a kdo bude odpovědný za správu těchto aplikací. Uživatelé musí mít nástroje pro kontrolu, jaká data chtějí zveřejnit, a musí si být vědomi toho, jak budou data použita.

2.4.3.1 Zabezpečení uložení dat

Pro bezpečné a přehledné ukládání dat je potřeba, aby data byly vhodně zpracovány a přizpůsobeny. Obecně koncová zařízení IoT mohou shromažďovat redundantní a nepřesná data. Proto nezpracovaná data nejsou vhodná k uložení. Konečným cílem ukládání dat v cloudu je jejich opětovné použití v budoucnosti, a proto je pro uživatele dat nezbytným požadavkem efektivní a přesné vyhledávání konkrétních dat. Z důvodu zabezpečení musíme zajistit důvěrnost dat bez zjevného snížení použitelnosti. Musíme tedy vědět, že dochází k ukládání validních dat a že nedošlo k jejich změně z třetí strany. Proto by měly být používány prvky k zajištění bezpečného ukládání dat. Vzhledem k tomu, že data jsou dynamicky shromažďována a některá nová data mohou být generována

v budoucnu, musí být data v cloudu organizována dynamicky a mezitím musí indexová struktura také podporovat dynamickou aktualizaci.

Studie [83] se zabývá návrhem, jak zabezpečit ukládání dat. Pro správné a bezpečné uložení dat je potřeba využívat zabezpečenou infrastrukturu, která se využívá šifrování dat. Každé koncové zařízení v síti musí být tedy správně připojené a musí znát potřebný klíč pro komunikaci. To zamezí napadení sítě vložením falešných koncových zařízení. Z koncových zařízení se data zasílají na edge server, neboli okrajový server, který má v tomto případě za úkol data rozšifrovat a zpracovat podle přednastavených pokynů. Následně jsou data opět zašifrována a zasílají se do cloudu.

3 Zhodnocení

Internet věcí se v dnešní době využívá ve většině oblastí, a to od dopravy, přes zdravotnictví, až po běžné domácnosti. Všechno napovídá tomu, že v blízké budoucnosti tomu nebude jinak. Naopak se obecně předpokládá, že se počet jeho aplikací několikanásobně poroste. Jak z této práce vyplývá, internet věcí s sebou přináší obrovská rizika. A to jsou kybernetické a fyzické útoky na tyto systémy. V poslední době, kdy je internet věcí stále více využíván pro zefektivnění rozsáhlých a důležitých infrastruktur, myslím, že bezpečnost těchto systémů se stává více důležitou.

Možných útoků již dnes existuje mnoho, a způsobů jak se proti nim bránit také. V případě, že je útok úspěšný, je důležité, jaké napáchá škody. Může jít pouze o zničení zařízení v podobě senzoru, získání neoprávněného přístupu do budovy, nebo získání cenných informací. Jako ukázka toho, jaké hrozí nebezpečí v případě používání IoT ve velkých infrastrukturách, nám může sloužit případ z roku 2015, kdy pouze jako ukázku nabourala dvojice odborníků řídící jednotku automobilu JEEP. Nenastala díky tomu žádná nebezpečná situace, ale bylo prokázáno, že zabezpečení IoT systému nebylo při výrobě bráno vozidla v potaz. Myslím, že není těžké si představit, co by se mohlo stát, kdyby se takovýto útok opakoval na běžně používaný automobil, nebo dokonce na větší počet automobilů. Jelikož dnes začínají být osobní i nákladní auta ovlivněné IoT ještě více, než v roce 2015, následky takového útoku mohou být kritické. V globálním měřítku, jsou ale takovéto útoky poměrně „neškodné“. Z globálního měřítka jsou větším problémem útoky realizované IoT Botnety. Příkladem může být útok IoT botnetem na společnost Dyn v roce 2016, kdy byly vyřazeny služby jako Reddit, Twitter, Netflix a mnoho dalších. I Když

tento útok neměl tak katastrofický dopad, vnímaly ho miliony lidí po celém světě, jelikož k těmto službám na určitou dobu ztratili přístup. Další případ útoku na IoT je napadení casina, kdy byly odcizeny informace o zákaznících.

IoT zařízení často postrádají dostatečné zabezpečení a většina současných výrobců neklade na jejich zabezpečení dostatečný důraz. Běžní spotřebitelé také nejsou o kyber-bezpečnosti výrobků dostatečně informováni. Tuto situaci by mohlo pomoci zlepšit zavedení bezpečnostního indexu [84] kterým by mohlo být v budoucnu každé IoT zařízení označené. Index v podobě nalepeného štítku na zařízení by běžným uživatelů jasně a stručně sdělil, jaké má dané zařízení zabezpečení.

Vzhledem k různorodosti aplikací IoT je potřeba přistupovat k zabezpečení více individuálně, protože každá aplikace vyžaduje jiný způsob zabezpečení a je třeba řešit zabezpečení ve všech vrstvách daného systému. Je ale také třeba dbát na bezpečnost ve všech vrstvách IoT.

Zabezpečení se velmi liší podle konkrétních aplikací. Například u velkých společností, které využívají inteligentní průmyslové systémy, dochází při úspěšném napadení třetí stranou k obrovským finančním ztrátám a je logické, že v tomto odvětví se do zabezpečení investuje nejvíce financí.

Pro zlepšení bezpečnosti internetu věcí v budoucnu, podle mého názoru, bude přispívat hlavně navýšení výpočetního výkonu na zařízení internetu věcí, což umožní dokonalejší metody šifrování.

Závěr

Účelem této práce bylo seznámit s problematikou bezpečnosti v oblasti internetu věcí. První kapitola se věnuje seznámení s internetem věcí, kde je krátce popsána jeho historie a také vize, kam do budoucna může tato technologie směřovat. Dále je popsána obecná architektura a také využití internetu věcí. V druhé kapitole je popsána bezpečnost internetu věcí. Je zde vysvětleno proč je nutné zabezpečovat internet věcí a také problémy, které mohou při využívání této technologie nastat. Tato kapitola také uvádí reálné útoky, které se v minulosti odehráli, a dále popisuje zabezpečení jednotlivých vrstev podle obecné architektury. V poslední kapitole je uvedeno konečné zhodnocení této problematiky

Seznam literatury a informačních zdrojů

[1] "That 'Internet of Things' Thing - 2009-06-22 - Page 1 - RFID Journal." [Online]. Dostupné na: https://www.rfidjournal.com/articles/view?4986. [Přidáno: 07-Mar-2019].

[2] "Internet of Things (IoT) History | Postscapes." [Online]. Dostupné na: https://www.postscapes.com/internet-of-things-history/. [Přidáno: 07-Mar-2019].

[3] "Internet of Things forecast – Ericsson Mobility Report - Ericsson." [Online]. Dostupné na: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast. [Přidáno: 20-Aug-2019].

[4] "• IoT: number of connected devices worldwide 2012-2025 | Statista." [Online]. Dostupné na: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Přidáno: 20-Aug-2019].

[5] Calum McClelland, "IoT Explained — How Does an IoT System Actually Work?" [Online]. Dostupné na: https://medium.com/iotforall/iot-explained-how-does-an-iot-system-actually-work-e90e2c435fe7. [Přidáno: 07-Mar-2019].

[6] Angela Karl, "Internet of Everything vs. Internet of Things." [Online]. Dostupné na: http://techgenix.com/internet-of-everything/. [Přidáno: 14-Aug-2019].

[7] Ahmed Banafa, "Internet of everything (IoE) - OpenMind." [Online]. Dostupné na: https://www.bbvaopenmind.com/en/technology/digital-world/the-internet-of-everything-ioe/. [Přidáno: 14-Aug-2019].

[8] I. Yaqoob *et al.*, "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," *IEEE Wirel. Commun.*, vol. 24, no. 3, pp. 10–16, Jun. 2017.

[9] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IOT applications," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 477–480.

[10] "IoT general architecture to data acquisition." [Online]. Dostupné na: https://www.researchgate.net/figure/IoT-general-architecture-to-data-acquisition_fig1_333123784. [Přidáno: 10-Jun-2019].

[11] Colin Geis, "Wireless or Wired Networking: Making the Best Choice For Industrial

Automation | FierceElectronics," 2018. [Online]. Dostupné na: https://www.fierceelectronics.com/iot-wireless/wireless-or-wired-networking-making-best-choice-for-industrial-automation. [Přidáno: 14-Aug-2019].

[12] Margaret Rouse, "What is Ethernet? - Definition from WhatIs.com." [Online]. Dostupné na: https://searchnetworking.techtarget.com/definition/Ethernet. [Přidáno: 14-Aug-2019].

[13] ALLEN JAME, "Wi-Fi vs. Ethernet: Which Connection to Use?," 2018. [Online]. Dostupné na: https://ubidots.com/blog/wi-fi-vs-ethernet-which-connection-to-use/. [Přidáno: 14-Aug-2019].

[14] "How Fast Is Ethernet Networking?" [Online]. Dostupné na: https://www.lifewire.com/how-fast-is-ethernet-817549. [Přidáno: 20-Aug-2019].

[15] T. Adame, A. Bel, B. Bellalta, J. Barcelo, and M. Oliver, "IEEE 802.11AH: the WiFi approach for M2M communications," *IEEE Wirel. Commun.*, vol. 21, no. 6, pp. 144–152, Dec. 2014.

[16] "11 Internet of Things (IoT) Protocols You Need to Know About." [Online]. Dostupné na: https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about. [Přidáno: 26-Apr-2019].

[17] "Top 7 Internet of Things IoT Communication Protocols | Breadware," 2011. [Online]. Dostupné na: https://breadware.com/blog/iot-communication-protocols/. [Přidáno: 26-Apr-2019].

[18] A. Augustin *et al.*, "A Study of LoRa: Long Range & Low Power Networks for the Internet of Things," *Sensors 2016, Vol. 16, Page 1466*, vol. 16, no. 9, p. 1466, Sep. 2016.

[19] "Mapy pokrytí – IoT portál," 2018. [Online]. Dostupné na: https://www.iot-portal.cz/mapa-pokryti/. [Přidáno: 26-Apr-2019].

[20] P. D. Ing. Michal Lom, prof. Ing. Ondřej Přibyl, "Sítě pro internet věcí v České republice," 2017. [Online]. Dostupné na: https://elektro.tzb-info.cz/informacni-a-telekomunikacni-technologie/16519-site-pro-internet-veci-v-ceske-republice. [Přidáno: 20-Aug-2019].

[21] "LoRaWAN™ Regional Parameters v1.1rB." [Online]. Dostupné na: https://lora-alliance.org/resource-hub/lorawantm-regional-parameters-v11rb. [Přidáno: 27-May-

2019].

[22] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Express*, vol. 3, no. 1, pp. 14–21, Mar. 2017.

[23] "IoT Plzeň." [Online]. Dostupné na: https://iot.plzen.eu/. [Přidáno: 26-Apr-2019].

[24] M. Bor and U. Roedig, "LoRa Transmission Parameter Selection," in *2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2017, pp. 27–34.

[25] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios," *IEEE Wirel. Commun.*, vol. 23, no. 5, pp. 60–67, Oct. 2016.

[26] S. Barrachina-Muñoz, B. Bellalta, T. Adame, and A. Bel, "Multi-hop communication in the uplink for LPWANs," *Comput. Networks*, vol. 123, pp. 153–168, Aug. 2017.

[27] "SIGFOX: nová bezdrátová síť pro „internet věcí" v České republice | T-Mobile t-press." [Online]. Dostupné na: http://www.t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/sigfox-nova-bezdratova-sit-pro-internet-veci-v-ceske-republice.html. [Přidáno: 27-Apr-2019].

[28] "Sigfox Technical Overview," 2017.

[29] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, Mar. 2019.

[30] "O2 | Internet věcí - IoT." [Online]. Dostupné na: https://www.o2.cz/firmy-a-organizace/it-reseni/iot. [Přidáno: 27-Apr-2019].

[31] "NB-IoT - Vodafone.cz." [Online]. Available: https://www.vodafone.cz/internet-veci/?tc=p_CZ_19_AO_P_M_J_A_G_DSA&gclid=EAIaIQobChMIg9n9za_w4QIVyud3Ch2MYA05EAAYASAAEgIVE_D_BwE. [Přidáno: 27-Apr-2019].

[32] "What Is Cellular IoT? | IoT For All." [Online]. Dostupné na: https://www.iotforall.com/what-is-cellular-iot/. [Přidáno: 27-Apr-2019].

[33] "Budoucnost internetu – IoT, 5G, konvergence." [Online]. Dostupné na: http://www.abclinuxu.cz/clanky/budoucnost-internetu-iot-5g-konvergence.

[Přidáno: 27-Apr-2019].

[34] "What is an IoT Gateway? - A Simple Explanation | IoT For All." [Online]. Dostupné na: https://www.iotforall.com/what-is-a-gateway/. [Přidáno: 20-Aug-2019].

[35] "What is an IoT Gateway? | Open Automation Software." [Online]. Dostupné na: https://openautomationsoftware.com/blog/what-is-an-iot-gateway/. [Přidáno: 15-Aug-2019].

[36] "LoRaWAN LPWAN network, devices and gateways - DPTechnics." [Online]. Dostupné na: https://www.dptechnics.com/en/technology/lora-wan.html. [Přidáno: 15-Aug-2019].

[37] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition."

[38] "What is the Cloud? How Does it Fit into the Internet of Things (IoT)? | IoT For All." [Online]. Dostupné na: https://www.iotforall.com/what-is-the-cloud/. [Přidáno: 07-Mar-2019].

[39] Petr Krčmář, "Mozilla se vrací k IoT projektem Things Gateway, bez cloudu a u vás doma - Root.cz," 2018. [Online]. Dostupné na: https://www.root.cz/clanky/mozilla-se-vraci-k-iot-projektem-things-gateway-bez-cloudu-a-u-vas-doma/. [Přidáno: 25-Apr-2019].

[40] H.-L. Truong and S. Dustdar, "Principles for Engineering IoT Cloud Systems," *IEEE Cloud Comput.*, vol. 2, no. 2, pp. 68–76, Mar. 2015.

[41] "Cloud Computing : IaaS, SaaS, PaaS for Internet of Things (IoT), Artificial Intelligence, Machine Learning and Scalable Digital Applications - Dihuni." [Online]. Dostupné na: https://www.dihuni.com/cloud-computing-iaas-saas-paas-for-internet-of-things-iot-artificial-intelligence-machine-learning-and-scalable-digital-applications/. [Přidáno: 15-Aug-2019].

[42] "What Is Cloud Computing? A Beginner's Guide | Microsoft Azure." [Online]. Dostupné na: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/. [Přidáno: 20-Aug-2019].

[43] "Co je SaaS? Software jako služba | Microsoft Azure." [Online]. Dostupné na: https://azure.microsoft.com/cs-cz/overview/what-is-saas/. [Přidáno: 15-Aug-2019].

[44] "Directory of Azure Cloud Services | Microsoft Azure." [Online]. Dostupné na: https://azure.microsoft.com/en-us/services/#iot. [Přidáno: 19-Aug-2019].

[45] "Amazon Web Services (AWS) - Cloud Computing Services." [Online]. Dostupné na: https://aws.amazon.com/. [Přidáno: 19-Aug-2019].

[46] "IoT Home Guide | 2019 Overview of the Best Connected Home Products." [Online]. Dostupné na: https://www.postscapes.com/internet-of-things-award/connected-home-products/. [Přidáno: 08-Mar-2019].

[47] "Chytrá domácnost: Výhody, možnosti a rizika inteligentních domů | Nazeleno.cz." [Online]. Dostupné na: https://www.nazeleno.cz/bydleni/chytra-domacnost-vyhody-moznosti-a-rizika-inteligentnich-domu.aspx. [Přidáno: 08-Mar-2019].

[48] K. A. Hribernik, Warden, Tobias, K.-D. Thoben, Herzog, and Otthein, "AN INTERNET OF THINGS FOR TRANSPORT LOGISTICS-AN APPROACH TO CONNECTING THE INFORMATION AND MATERIAL FLOWS IN AUTONOMOUS COOPERATING LOGISTICS PROCESSES."

[49] B. Karakostas, "A DNS Architecture for the Internet of Things: A Case Study in Transport Logistics," *Procedia Comput. Sci.*, vol. 19, pp. 594–601, Jan. 2013.

[50] "Smart tracking - IoT.smart - Nový svět IoT." [Online]. Dostupné na: https://www.iotsmart.cz/smarttracking. [Přidáno: 08-Mar-2019].

[51] N. Gondchawar and R. S. Kawitkar, "IJARCCE IoT based Smart Agriculture," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, 2016.

[52] K. Natarajan, "Smart Health Care System Using Internet of Things," *J. Netw. Commun. Emerg. Technol. www.jncet.org*, vol. 6, 2016.

[53] P. Raga Lavima and M. G. Subhramanya Sarma, "International Journal of Computer Science and Mobile Computing AN IOT BASED INTELLIGENT MEDICINE BOX," 2015.

[54] "IoT Technology in the Energy Sector." [Online]. Dostupné na: https://internet-of-things-innovation.com/insights/the-blog/iot-technology-energy-sector/#.XOu87IgzZPY. [Přidáno: 27-May-2019].

[55] P. Neirotti, A. De Marco, A. C. Cagliano, G. Mangano, and F. Scorrano, "Current trends in Smart City initiatives: Some stylised facts," *Cities*, vol. 38, pp. 25–36, Jun.

2014.

[56] T. Shelton, M. Zook, and A. Wiig, "The 'actually existing smart city,'" *Cambridge J. Reg. Econ. Soc.*, vol. 8, no. 1, pp. 13–25, Mar. 2015.

[57] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[58] "What is Smart City." [Online]. Dostupné na: http://smartcities.gov.in/content/innerpage/what-is-smart-city.php. [Přidáno: 29-May-2019].

[59] Centre for Cities, "Smart cities definitions," 2014. [Online]. Dostupné na: https://www.centreforcities.org/reader/smart-cities/what-is-a-smart-city/1-smart-cities-definitions/. [Přidáno: 29-May-2019].

[60] D. V Jose and A. Vijyalakshmi, "An Overview of Security in Internet of Things," *Procedia Comput. Sci.*, vol. 143, pp. 744–748, Jan. 2018.

[61] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[62] M. binti Mohamad Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Networks*, vol. 148, pp. 283–294, Jan. 2019.

[63] "When good IoT devices go bad | HPE." [Online]. Dostupné na: https://www.hpe.com/us/en/insights/articles/when-good-iot-devices-go-bad-1707.html. [Přidáno: 01-Aug-2019].

[64] "Black Hat USA 2015: The full story of how that Jeep was hacked | Kaspersky official blog." [Online]. Available: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/. [Přidáno: 01-Aug-2019].

[65] "What is a DDoS Botnet? | Cloudflare." [Online]. Dostupné na: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/. [Přidáno: 07-Aug-2019].

[66] Nicky Wolf, "DDoS attack that disrupted internet was largest of its kind in history, experts say | Technology | The Guardian," 2016. [Online]. Available:

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet. [Přidáno: 21-May-2019].

[67] Jessica Miley, "A Casino's Database Was Hacked Through A Smart Fish Tank Thermometer," 2018. [Online]. Dostupné na: https://interestingengineering.com/a-casinos-database-was-hacked-through-a-smart-fish-tank-thermometer. [Přidáno: 20-Aug-2019].

[68] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[69] Y. Yao, L. T. Yang, and N. N. Xiong, "Anonymity-Based Privacy-Preserving Data Reporting for Participatory Sensing," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 381–390, Oct. 2015.

[70] D. Karaklajic, J.-M. Schmidt, and I. Verbauwhede, "Hardware Designer's Guide to Fault Attacks," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 21, no. 12, pp. 2295–2306, Dec. 2013.

[71] Y. Li, M. Chen, and J. Wang, "Introduction to side-channel attacks and fault attacks," in *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, 2016, pp. 573–575.

[72] Jan Bělohoubek, "Zvyšování spolehlivosti a bezpečnosti číslicových obvodů na úrovni mikroarchitektury."

[73] R. Metz, "Finding insecurity in the internet of things," *Technol. Rev.*, vol. 119, no. 2, pp. 76–77, 2016.

[74] "WiFi Security - The Ultimate Guide." [Online]. Dostupné na: https://www.purevpn.com/wifi-vpn/security-protocols. [Přidáno: 18-Aug-2019].

[75] "Ransomware and Your Smart Home - The Security of Z-Wave." [Online]. Dostupné na: https://buildyoursmarthome.co/home-automation/protocols/security-of-z-wave-protocol/. [Přidáno: 19-Aug-2019].

[76] "Z-Wave's S2 Framework Provides Advanced IoT Security for the Smart Home - CE Pro," 2015. [Online]. Dostupné na: https://www.cepro.com/article/z_waves_s2_framework_provides_advanced_iot_security_for_the_smart_home. [Přidáno: 19-Aug-2019].

[77] "Security in ZigBee communications | INCIBE-CERT," 2016. [Online]. Dostupné na: https://www.incibe-cert.es/en/blog/security-zigbee-communications. [Přidáno: 18-Aug-2019].

[78] "Sigfox - The Global Communications Service Provider for the Internet of Things (IoT)." [Online]. Dostupné na: https://www.sigfox.com/en. [Accessed: 08-Aug-2019].

[79] "Security in LoRaWAN Applications – LPWAN LoRaWAN IoT Simplified," 2018. [Online]. Dostupné na: https://smartmakers.io/en/security-in-lorawan-applications/. [Přidáno: 08-Aug-2019].

[80] "The security of NB-IoT devices - Accent Systems." [Online]. Dostupné na: https://accent-systems.com/blog/security-of-nb-iot-devices/. [Přidáno: 12-Aug-2019].

[81] "How Encryption is Powering the Future of IoT | IoT For All," 2018. [Online]. Dostupné na: https://www.iotforall.com/future-iot-encryption/. [Přidáno: 12-Aug-2019].

[82] "Top 5 encryption algorithms for IoT." [Online]. Dostupné na: https://ubidots.com/blog/top-5-encryption-algorithms-for-iot/. [Přidáno: 12-Aug-2019].

[83] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, "Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing," *IEEE Trans. Ind. Informatics*, vol. 14, no. 10, pp. 4519–4528, Oct. 2018.

[84] J. M. Blythe and S. D. Johnson, "The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices," pp. 4 (7 pp.)-4 (7 pp.), 2018.