Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Nástroje pro správu IoT zařízení

Jan Novotný

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jan Novotný

Informatika

Název práce

Nástroje pro správu IoT zařízení

Název anglicky

Tools for IoT device managment

Cíle práce

Bakalářská práce je tematicky zaměřena na problematiku hromadné správy zařízení internetu věcí.
Cílem práce je podle vybraných kritérií porovnat a zhodnotit nástroje pro správu IoT zařízení.
Mezi vedlejší cíle práce patří:
- charakterizovat problematiku správy IoT zařízení
- analyzovat požadavky na správu IoT zařízení
- zhodnotit jednotlivé vybrané nástroje

Metodika

Teoretická část práce je založena na analýze odborných zdrojů zabývajících se problematikou správy IoT zařízení.

V praktické části budou definovány požadavky na správu IoT zařízení

Následně budou vybrány vhodné nástroje pro správu IoT zařízení, které budou zhodnoceny.

Na základě syntézy těchto poznatků budou zpracovány závěry bakalářské práce.

Doporučený rozsah práce

30-40 stran

Klíčová slova

IoT, IT trendy, aplikace, budoucnost, inovace, bezpečnost

Doporučené zdroje informací

KLEIN, Scott, 2017. IOT solutions in Microsoft's Azure IOT Suite: Data Acquisition and Analysis in the real world. United States: Apress.

ROSSMAN, John, 2016. The amazon way on IOT: 10 principles for every leader from the world's leading internet of things strategies. B.m.: Clyde Hill Publishing.

TAMBOLI, 2019. Build your own IOT platform. B.m.: Apress.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Michal Stočes, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 7. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 07. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Nástroje pro správu IoT zařízení" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2024 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Michalovi Stočesovi, Ph.D. za vedení bakalářské práce, čas, spolupráci a cenné rady při vypracování.

Nástroje pro správu IoT zařízení

Abstrakt

Bakalářská práce se zaměřuje na analýzu a hodnocení nástrojů používaných pro správu a řízení internetu věcí zařízení. S rostoucím počtem a složitostí IoT zařízení v dnešním propojeném světě je klíčové mít efektivní nástroje pro jejich správu, monitorování a optimalizaci výkonu.

Cílem práce je porovnat a zhodnotit nástroje pro správu IoT zařízení na základě vybraných kritérií.

Vedlejšími cíli jsou charakterizace problematiky správy IoT zařízení, analýza požadavků na správu těchto zařízení a zhodnocení vybraných nástrojů. Teoretická část vychází z analýzy odborných zdrojů, zatímco praktická část definuje požadavky, vybírá nástroje a hodnotí je. Získané poznatky jsou syntetizovány v závěrech práce.

Klíčová slova: IoT, IoT trendy, aplikace, budoucnost, inovace, bezpečnost

Tools for IoT device management

Abstract

This bachelor thesis focuses on the analysis and evaluation of tools used to manage and control internet of things devices. With the increasing number and complexity of IoT devices in today's connected world, it is crucial to have effective tools to manage, monitor and optimize their performance. The aim of this thesis is to compare and evaluate IoT device management tools based on selected criteria. The secondary objectives are to characterize the issues involved in IoT device management, analyse the requirements for managing these devices, and evaluate the selected tools. The theoretical part is based on the analysis of expert sources, while the practical part defines requirements, selects tools, and evaluates them. The obtained knowledge is synthesized in the conclusions of the thesis.

Keywords: IoT, IoT trends, application, future, innovation, security

Obsah

1 Úvod

Dnes když jsou téměř všechna zařízení připojená k internetu a jejich počet stále roste, je nutné o těchto zařízení vědět všechny informace se zabezpečeným přístupem, a to s co nejmenší prodlevou a zároveň přehledně, a to třeba i z mobilního telefonu.

Jedním z klíčových hledisek, které hraje roli při výběru onoho nástroje pro správu IoT zařízení je škálovatelnost. Škálovatelnost je schopnost přizpůsobit se a efektivně reagovat na náhle změny potřeb systému.

Tato práce se věnuje problematice hromadné správy IoT zařízení a taktéž vybráním tzv. kompresního řešení pomocí metody AHP, kde kompromisní řešení představuje jeden optimální nástroj nebo platformu podle stanovených kritériích.

2 Cíl práce a metodika

2.1 Cíle práce

Bakalářská práce je tematicky zaměřena na problematiku hromadné správy zařízení internetu věcí. Cílem práce je podle vybraných kritérií porovnat a zhodnotit nástroje pro správu IoT zařízení. Mezi vedlejší cíle práce patří:

- charakterizovat problematiku správy IoT zařízení
- analyzovat požadavky na správu IoT zařízení
- zhodnotit jednotlivé vybrané nástroje

2.2 Metodika

Teoretická část práce je založena na analýze odborných zdrojů zabývajících se problematikou správy IoT zařízení. V praktické části budou definovány požadavky na správu IoT zařízení. Následně budou vybrány vhodné nástroje pro správu IoT zařízení, které budou zhodnoceny. Na základě syntézy těchto poznatků budou zpracovány závěry bakalářské práce.

3 Teoretická východiska

3.1 Internet věcí

Žádná unikátní definice internetu věcí neboli IoT, která by byla přijata celkovou světovou komunitou uživatelů jednoduše neexistuje. Naopak existuje mnoho odlišných skupin, mezi nimiž jsou akademici, výzkumníci, praktici, inovátoři a vývojáři, kteří tento termín definovali podle sebe, ačkoli jeho prvotní použití se připisuje Kevinu Ashtonovi, který tento pojem poprvé pronesl v roce 1999. (Madakam, et al., 2015)

Jako nejlepší definici internetu věcí lze označit jako otevřenou a komplexní síť inteligentních objektů, které mají schopnost samy se organizovat, sdílet informace, data a zdroje, reagují a jednají v závislosti na situacích a změnách v prostředí. (Madakam, et al., 2015)

Z technického hlediska se internet věcí skládá z rostoucího počtu senzorů po celém světě, které shromažďují a přenášejí data. internet věcí se také vztahuje k pravidlům a událostem, které se na tato data aplikují za účelem úprav systémů a organizací. (Rossman, 2016)

3.1.1 Architektura internetu věcí

Vytvoření co možná nejlepšího návrhu architektury je prvotním krokem pro vybudování privilegovaného systému IoT. Tato architektura pomohla vyřešit mnoho problémů v prostředí IoT, jako je škálovatelnost, směrování, síťování a mnoho dalších. Přístup k architektuře IoT je typicky založen na třech hlavních aspektech. Průnik těchto aspektů vytváří nový prostor nazvaný „infrastruktura internetu věcí“. (Ali, et al., 2015)

a) Informační prvky (Information items) – jedná o všechny prvky připojené k prostředí IoT.
b) Nezávislá síť (Independent network) – zahrnuje několik funkcí jako je samokonfigurace, vlastní ochrana, vlastní přizpůsobení a vlastní optimalizace.
c) Inteligentní aplikace (Intelligent applications) – takové aplikace, které mají inteligentní řízení, metody výměny a zpracování dat.

3.1.2 Rozdíly mezi internetem věcí a tradiční sítí

Zpočátku technologie internetu věcí narušila řadu zaběhnutých koncepcí sítí a zahájila novou éru telekomunikačních technologií. IoT lze považovat za rozšíření a expanzi internetu. (Ali, et al., 2015)

Internet věcí nemusí nutně používat IP ve všech případech pro adresování zařízení, protože povaha internetu věcí vyžaduje odlehčené komunikační protokoly, tudíž komplexita TCP/IP protokolu není vhodná zejména při práci se chytrými zařízeními. (Ali, et al., 2015)

IoT prostředí je na rozdíl od tradiční sítě založeno především na připojených chytrých zařízeních. Tyto zařízení jsou důležitým aspektem, které z internetu věcí činí více než pouhé rozšíření internetu. Takové chování IoT závisí na vytvoření interoperabilních systémů. (Ali, et al., 2015)

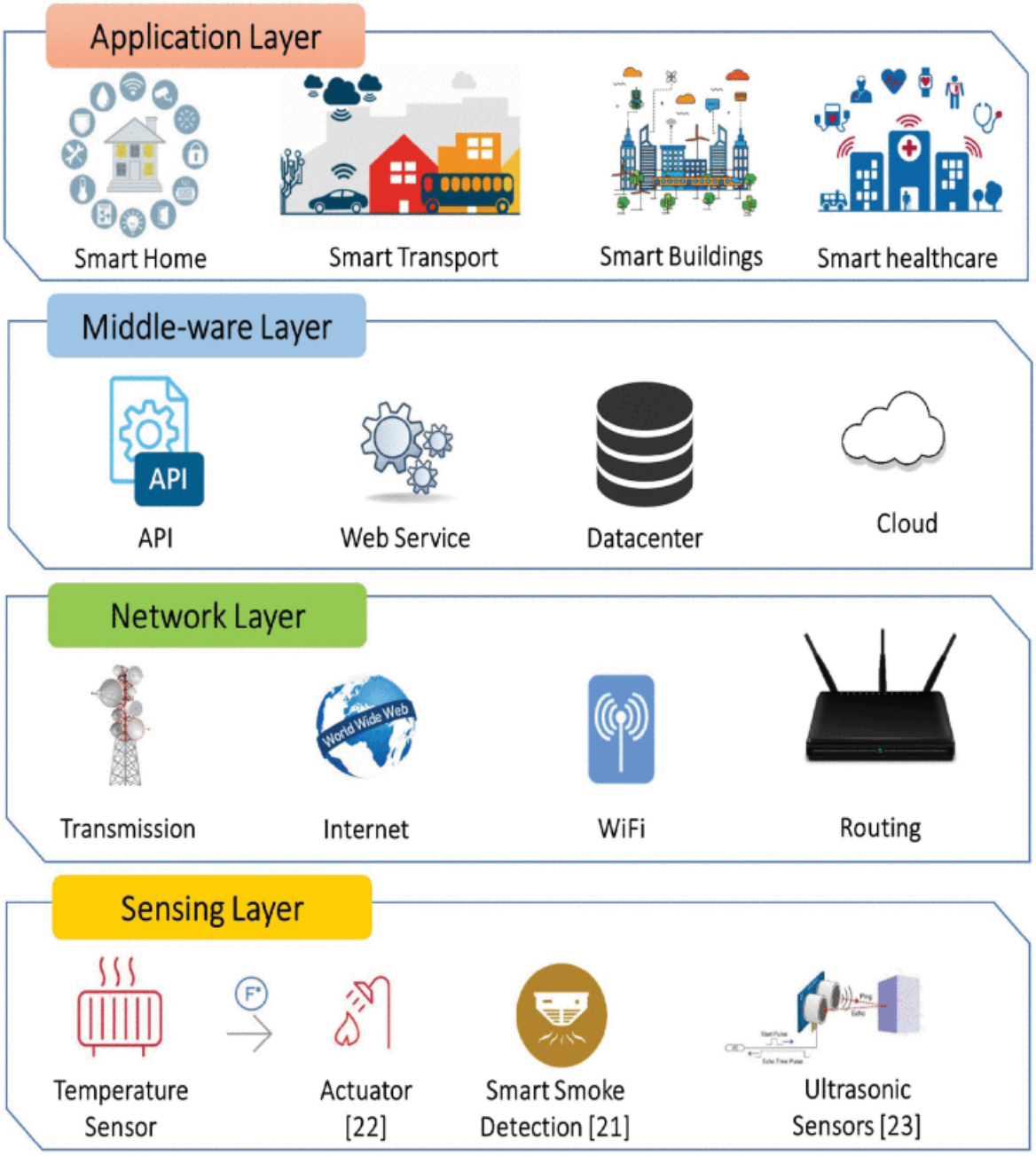
Z předchozích tvrzení lze představit rovnici představující IoT. internet věcí = internet + WSN (Bezdrátová senzorová síť) + Chytré prvky obklopené chytrým prostředím. (Ali, et al., 2015)

3.1.3 Vrstvy IoT prostředí

IoT aplikace se může rozdělit do čtyř základních vrstev. Každá z těchto vrstev používá širokou škálu technologií viz. Obrázek 1 - Vrstvy IoT aplikace. (Hassija, et al., 2019)

1. Sensing layer (Snímací vrstva) – zahrnuje využití různých senzorů a akčních členů k snímaní dat nebo informací pro provádění různých funkcionalit.
2. Network layer (Síťová vrstva) – zde probíhá přenos shromážděných dat přes komunikační síť.
3. Middleware layer (Middleware vrstva) – většina IoT aplikací se nasazuje na této vrstvě.

4. Application layer (Aplikační vrstva) – na této vrstvě se provozují už konkrétní end-to-end aplikace.



Obrázek 1 - Vrstvy IoT aplikace

3.1.4 Technologický řetězec internetu věcí

Mezi klíčové technologie většiny IoT řešení patří senzory, konektivita, cloudové ukládání a zpracování dat, analytika a strojové učení. Každá z těchto technologií dělá rychle pokroky ve schopnostech, nákladech, provozní vhodnosti, standardizaci a snadnosti vývoje a nasazení. Architektury pro rozsáhlá IoT nasazení pokračují v rychlém vývoji. Vždy existují kompromisy mezi rychlostí, odolností, náklady a provozní údržbou pro rozsáhlé množství zařízení obsahující senzory. Tento technologický řetězec samozřejmě není jednosměrný, upozornění, data a úpravy proudí zpět do zařízení. viz. Obrázek 2 - Technologický řetězec internetu věcí (Rossman, 2016)

Senzory a zařízení

Senzory a zařízení nejsou jen místem, kde se data nebo události zachycují, ale často zde také probíhá významná část zpracování. Operační systémy, software, napájení, senzory zachycující data nebo události jsou klíčové technologické součásti, které se často nacházejí přímo v samotném zařízení. (Rossman, 2016)

Tato zařízení jsou kritickými uzly aplikací IoT a musí poskytovat plnou funkčnost řešení tím, že fungují jako vstupy, výstupy. (Tamboli, 2022)

Konektivita

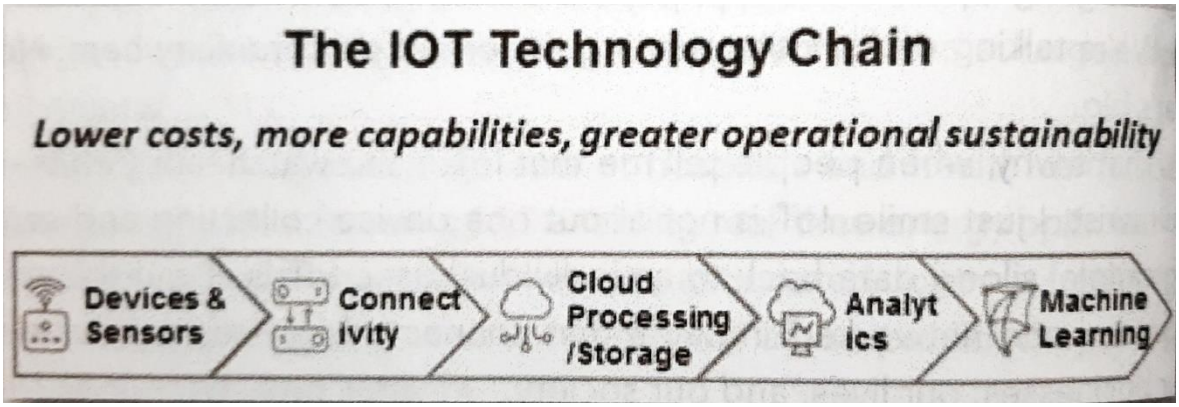
Konektivita je široký soubor možností připojení zařízení ke cloudu nebo jiným zařízením. Existuje mnoho možností, z nichž každá má vlastní aspekty. K dispozici jsou technologie RFID, Bluetooth, bezdrátové nebo drátové připojení, a to jsou jen některé z nich. Výkon, spotřeba energie, náklady a provozní vhodnost se v jednotlivých technologiích značně liší. (Rossman, 2016)

Cloud

Cloud poskytuje rozšiřitelné centrální prostředí pro zpracování a ukládání dat. V cloudovém prostředí hraje roli geografická povaha situace, požadavky na rychlost a zpracování v reálném čase a také objem a rozmanitost dat. Typicky se v cloudovém prostředí nachází řešení pro analýzu, správu události a dat, která jsou potřebná pro IoT řešení. To zahrnuje databázové požadavky, notifikace událostí, vizualizaci dat a nástroje pro vytváření zpráv. (Rossman, 2016)

Strojové učení

Poslední součástí je strojové učení a jeho algoritmy. Jedná se o algoritmy učení, které rozpoznávají klíčové optimalizace a úpravy, jež je třeba v zařízeních provést. Tato komponenta se nachází v cloudu, nebo přímo v zařízeních. (Rossman, 2016)



Obrázek 2 - Technologický řetězec internetu věcí

3.2 Síťování internetu věcí

Obecně platí, že problematika síťování je závažným tématem, protože zahrnuje jen některé důležité faktory, které se uplatňují při správě sítí. Především se jedná o datové přenosy a protokoly, které mají významný dopad na chování celé sítě. V IoT sítích nelze předvídat, kde se objekt nachází, nebo zda potřeba objekt přenést do jiné sítě. Největší problém se nachází v dynamické změně bran a obtížné identifikaci polohy objektů. (Ali, et al., 2015)

MANET (Mobile Ad-hoc network) je síť skládající se z několika samoorganizovaných mobilních uzlů nebo objektů a je považována za způsob udržení spojení a také za rozšíření stávající infrastruktury v IoT. (Ali, et al., 2015)

3.3 Směrování internetu věcí

Zabývá se výběrem nejlepší cesty mezi zdrojem a cílem pro úspěšné dokončení komunikačního procesu. Existují různé způsoby určení nejlepší cesty podle typu komunikačního protokolu, jako je počet skoků, náklady a šířka pásma. (Ali, et al., 2015)

Může být směrovací protokoly rozdělit do dvou hlavních kategorií:

- Reaktivní protokoly: cesta je stanovena po zadání požadavku na přenos,
- Proaktivní protokoly: počáteční cesta před odesláním požadavku.

3.4 Různorodost internetu věcí

IoT prostředí je nejznámějším příkladem reprezentujícím problematiku heterogenity, protože obsahuje množství různých zařízení; hlavním cílem internetu věcí je vytvořit společný způsob abstrakce heterogenity těchto zařízení a dosáhnout optimálního využití jejich funkcí. (Ali, et al., 2015)

Middleware vrstva je softwarová vrstva nebo sada dílčích vrstev umístěných mezi technologickou a aplikační vrstvou, která poskytuje standardní způsob reprezentace dat a komunikace. Obecně tato vrstva podporuje koncept transparentnosti, který se používá ke skrytí všech komplexních detailů před koncovým uživatelem. Koncept transparentnosti je vlastně jednou z nejvýznamnějších vlastností distribuovaných systémů. Architektura orientovaná na služby je běžným příkladem middlewarové technologie, která se používá pro IoT řešení. (Ali, et al., 2015)

Middleware se skládá ze tří hlavních vrstev:

a) Vrstva pro kompozici služeb
b) Vrstva správy služeb
    - Tato vrstva zahrnuje služby jako je dynamická identifikace objektů, monitorování, vynucování politiky služeb.
    - Runtime – služby, které jsou založeny na čase jako rozhodujícím faktoru pro jejich přímou implementaci
    - Design time – služby, které jsou součástí životního cyklu
c) Vrstva abstrakce objektů
    - Tato vrstva organizuje přístup k různorodým zařízením pomocí společného jazyka.
    - Podvrstva rozhraní – spravuje příchozí a odchozí zprávy

- Podvrstva komunikační – implementuje logiku u metod webové služby a překládá tyto metody u zařízení pro komunikaci s objekty reálného světa

3.5 Interoperabilita internetu věcí

Pojem interoperabilita lze definovat jako schopnost vytvářet systémy nebo zařízení, které spolu efektivně komunikují. Smart-M3 architektura spočívá v rozdělení IoT prostředí na malé části, které usnadňují proces jejich správy. (Ali, et al., 2015)

3.6 Kvalita poskytnutých služeb internetu věcí

V ideálním případě je QoS definována jako „doba za kterou je zpráva doručena od odesílatele k příjemci“ a tato doba musí být menší nebo rovna než předem časový požadavek. (Ali, et al., 2015)

Internetové služby lze klasifikovat podle modelů internetových služeb, které umožňují kategorizovat internetové aplikace podle priority a stanoví požadavky na QoS nezbytné pro dosažení spokojenosti uživatelů. (Ali, et al., 2015)

Modely služeb se skládají ze tří faktorů

a) Prodleva
    1. Hard Real Time
    2. Soft Real Time
    3. Non-Real Time
b) Faktora citlivosti aplikace
c) Faktor interaktivity

3.7 Škálovatelnost internetu věcí

Škálovatelnost je schopnost systému nebo sítě zvládnout rostoucí rozsah jakéhokoli prostředí bez ovlivnění výkonu a jednou z nejdůležitějších výzev IoT. (Ali, et al., 2015)

Je to základní vlastnost každého systému, který je schopen zvládnout rostoucí množství práce. Nedostatek této vlastnosti může způsobit nedostatečnou výkonnost systému a nutnost reorganizace celého systému. (Gupta, et al., 2017)

Hlavním cílem škálovatelnosti zařízení je vyhovět měnícím se požadavkům, které nikdy nemohou být statické, protože zájem lidí a vkus se mění s časem a také s podmínkami prostředí. Je zásadní, protože přispívá ke konkurenceschopnosti, účinnosti a kvalitě. Důležitost škálovatelnosti spočívá v tom, že pomáhá v systému pracovat elegantně bez zbytečného zpoždění a neproduktivní spotřeby zdrojů a dobře využívá dostupné zdroje. V škálovatelném systému, pokud se požadavky na paměť systému zvyšují se zvyšujícím se množstvím dat, pak neroste na nepodporovanou úroveň. Zařízení navíc funguje hladce a rychle bez ohledu na to, zda je zařízení velké nebo malé. (Gupta, et al., 2017)

Funkce pro škálovatelnost

Škálovatelnost je poháněna menšími a více specializovanými procesy. Funkce, které je důležité mít na paměti jsou např. marketing, hardware, software a síť. (Gupta, et al., 2017)

Techniky pro škálovatelnost

Zařízení nebo systém můžou být škálovatelné různými způsoby. K dosáhnutí neomezené škálovatelnosti, se musí dodržovat správně sestavenou řadu kroků, které usnadní škálovatelnost usnadní. (Gupta, et al., 2017)

Výzkumné výzvy a problémy

Mezi nejčastější výzvy a úskalí, které je nutné zvažovat, spadá protokolování, síťové zabezpečení, správa identit, soukromí, důvěra a správa, odolnost proti poruchám. Prostředí IoT propojuje obrovské množství senzorů, akčních členů a dalších zařízení, aby bylo možné sdílet informace a velké množství aplikací přes internet do jednoho celku. (Gupta, et al., 2017)

Vertikální škálovatelnost

Označuje se také jako „scaling up“, což je schopnost zvýšit kapacitu stávajícího hardwaru nebo softwaru přidáním dalších zdrojů. Serveru například přidáváme výpočetní výkon, aby byla zvýšena jeho rychlost. Mimo jiné systém může být vertikálně škálován přidáním více výpočetních prostředků, operační paměti, úložného prostoru a síťových rozhraní, aby byly uspokojeny narůstající požadavky na systém. Společnosti poskytující hostingové služby přidávají prostředky do jednoho uzlu systému, což zahrnuje přidání procesorů nebo paměti do jednoho počítače. Takové vertikální škálování současných systémů jim usnadňuje produktivnější využití technologie virtualizace. (Gupta, et al., 2017)

Horizontální škálovatelnost

Používá se také termín „scaling out“, který představuje možnost zvýšit kapacitu připojením více hardwarových nebo softwarových entit, tak aby mohly spolupracovat jako jeden celek. Horizontální škálovatelnosti lze dosáhnout přidáním dalších zařízeních do skupiny zdrojů a přidáním více uzlů do systému, například přidáním nového počítače do distribuované softwarové aplikace. (Gupta, et al., 2017)

Příkladem mohou být systémy s architekturou orientovanou na služby a webové servery, které škálují pomocí přidáváním dalších serverů do sítě s vyváženou zatížeností tak, aby se příchozí požadavky mohly být rozděleny mezi všechny. (Gupta, et al., 2017)

Cluster je známý termín, používaný pro popis „scaling out“ systému. Příkladem může být přechod z jednoho systému webového serveru na další tři systémy. Systémoví architekti mohou sestavit roj malých počítačů v clusteru, aby získali kumulativní výpočetní výkon, který mnohonásobně převyšuje výkon počítačů založených na jediném tradičním procesoru. (Gupta, et al., 2017)

Použití automatizovaného bootstrappingu

S rostoucím počtem zařízení již není možné provádět manuální funkce, jako je zavádění, konfigurace softwaru a zabezpečení, registrace a aktualizace zařízení. Jakýkoli mechanismus, který zahrnuje lidskou interakci a usnadnění, tak začíná být zastaralý a nepraktický. Proto musí všechny tyto služby výše uvedené procesy automatizovat, aby ušetřily čas a jednaly efektivněji. Zařízení musí mít vestavěná zařízení s požadovanými zavaděči, bezpečnostními klíči a dalšími nezbytnými funkcemi, které podpoří proces automatizaci při prvním spuštění vzdáleného zařízení. (Gupta, et al., 2017)

Řízení IoT datového toku

Zařízení internetu věcí generují a přenášejí obrovské množství dat, která je třeba zpracovat a uspořádat do požadovaného formátu, aby byla použitelná. V IoT aplikacích je nezbytně nutný datový tok, který se skládá ze shromážděných front-endů a specifické sady funkcí pro správu dat a obsahu. Obsažené funkce jsou vhodně aplikovány na datový tok, který je přenášen mezi různými systémy a zařízeními. S rostoucím počtem zařízení, která se podílejí na generování a přenosu dat, musí být tento datový tok navržen tak, aby zvládl náhlý nárůst rychlosti toku dat a problémy s výkonem. Kapacita těchto datových toků musí být přizpůsobena na základě cenných parametrů, jako je počet současně připojených zařízení

nebo datových toků. Proto je zásadní, aby v datovém toku existovala kontrola podle požadavků konkrétní služby. (Gupta, et al., 2017)

Tříosý přístup pro škálování

IoT aplikace lze škálovat podle tří základních os. Osa X představuje škálování klonováním, osa Y představuje škálování rozdělením různých prvků a osa Z představuje škálování rozdělením podobných prvků. Škálování na ose X je spojeno s využitím většího množství zdrojů k rozdělení příchozích požadavků mezi různé servery tak, aby všechny servery byly schopny požadavky vyřídit. Je výhodné začlenit servery, které zachovávají informace o stavu od jednoho požadavku k druhému. Takové servery lze snadno škálovat. Škálování v ose Y trvale znamená rozdělování daných úloh na základě procesů. Škálování v ose Z znamená rozdělování povinností na základě příchozích údajů o požadavcích nebo odpovědích. (Gupta, et al., 2017)

Vývoj architektury mikroslužeb

Mikroslužby jsou moderní architektonický přístup, v němž se složité aplikace skládají z jednotlivých mikroprocesů, které se mezi sebou šíří pomocí jazykově nezávislých rozhraní API. Každou aplikaci je vhodné rozdělit na několik nezávislých instancí, které se často nazývají funkční jednotky, z nichž každá vykonává samostatnou funkci. Každá z těchto funkčních jednotek by měla pracovat nezávisle a vykonávat se. Tyto funkční jednotky si mohou navzájem posílat zprávy. (Gupta, et al., 2017)

Zavedení více technologií ukládání dat

IoT prostředí má různé části aplikací, které vyžadují různé techniky pro jejich ukládání, místo aby se používala jedna společná technika pro všechny. Tyto aplikace je třeba postavit na nejvhodnějších technologických komponentách, které jsou k dispozici, a proto by každá z mikroslužeb, které budou používány, měla používat tu komponentu, která je vhodná pro její potřeby. Mimoto by měl dotaz na data a požadavky na vyhledávání určovat jejich volbu výběr databáze. (Gupta, et al., 2017)

Zabezpečení protokolů a sítí

Jako protokol se označuje především přístupová metoda, která je standardem pro definování schématu pro výměnu dat v různých počítačových sítích, jako je lokální počítačová síť (LAN), intranet, internet apod. S tím souvisí zřejmá naléhavost zabezpečení sítí proti různým nekalým praktikám. Zabezpečení protokolů a sítí je dominantním faktorem vedoucím ke škálovatelnosti, neboť s nárůstem počtu zařízení, které se připojují k internetu,

se musí definovat nové protokoly, které pojmou a na dálku identifikují každé zařízení. Proto je velmi důležité začlenit kryptografické algoritmy, které mohou zajistit vysokou propustnost. (Gupta, et al., 2017)

Důvěra a správa

Důvěra a správa jsou povinné pro realizaci důvěry mezi různými subjekty a také z pohledu uživatele. Pro získání důvěry ze strany uživatele musí internet věcí udržovat systém správy důvěry, který zajistí důvěru mezi uživatelem a systémem. Z hlediska systému je klíčová správa, kde by měly být obsaženy politiky a kde je postaráno o politiku vs. kontrolu. Pokud neexistuje řádný systém řízení důvěry, existuje možnost narušení důvěry mezi subjekty nebo mezi subjektem a věcí. (Gupta, et al., 2017)

Odolnost proti poruchám

Hlavním cílem odolnosti proti poruchám v IoT prostředí je snadno se přizpůsobit neustále se měnícímu prostředí a vytvořit spolehlivou redundanci. Vzhledem k tomu, že nyní miliardy zařízení vytvářejí a spotřebovávají služby, bude toto prostředí náchylnější k útokům. Právě nesmírně omezená zařízení budou nejvíce náchylná k útokům a škodlivé systémy se mohou pokusit získat kontrolu nad ostatními zařízeními buď přímo, nebo nepřímo. Z tohoto důvodu tedy může být tolerance vůči chybám pravděpodobným problémem v oblasti škálovatelnosti. (Gupta, et al., 2017)

Řízení přístupu

Takováto kontrola umožňuje přístup k různým zdrojům IoT prostředí pouze oprávněným uživatelům. Například administrátor bude mít širší přístup ve srovnání s běžnými uživateli. Vznikající technologie IoT vyžaduje zvláštní výzvy v oblasti řízení přístupu kvůli malé šířce pásma mezi zařízeními IoT a internetem, nízkým energetickým nárokům zařízení IoT a také kvůli distribuované architektuře, která se v systému uplatňuje. (Gupta, et al., 2017)

3.8 Virtualizace internetu věcí

Virtualizace je proces, který umožňuje efektivnější využití fyzického počítačového hardwaru a je základem cloud computingu. Virtualizace využívá software k vytvoření abstrakční vrstvy nad počítačovým hardwarem, která umožňuje rozdělit hardwarové prvky

jednoho počítače, jako jsou procesory, paměť, uložiště a jiné, na více virtuálních počítačů, běžně nazývaných virtuální stroje. (IBM, 2021)

Tato technologie umožňuje, aby na jednom serveru běželo více operačních systém nebo softwaru, jako jsou aplikace a služby, a to vytvořením více než virtuální stroje uvnitř fyzického počítač. (Ali, et al., 2015)

Framework „an IoT Virtualization Framework Based on Sensor as a service notion“ některé výzvy v IoT prostředí a se skládá ze čtyř vrstev: (Ali, et al., 2015)

a) Vrstva reálného světa
b) Sémantické vrstvy
c) Virtualizační vrstva
d) Samostatná databáze pro ukládání dat

Hlavní výzvy v IoT prostředí lze primárně rozdělit do tři položek: (Ali, et al., 2015)

a) Neexistující registr, framework disponuje databází, která by tuto výzvu překonala
b) Různorodost, navrhovaný framework se snažil překonat tento problém prostřednictvím sémantického přístupu k řešení heterogenity pomocí standardizovaného jazyka Sensor Model Language.
c) Chybějící interakce mezi událostí a službou, framework využívá virtualizační vrstvu k efektivnímu řešení této výzvy.

3.9 Big Data internetu věcí

Big Data je neologismus pro označení obrovského množství dat, ať už strukturovaných nebo nestrukturovaných, s nimiž je obtížné pracovat tradičními databázovými metodami a softwarovými technikami. Zjednodušeně lze Big Data definovat jako velký objem dat. Datová sada se považuje za Big Data, pokud splňuje 4 vlastnosti hodnotu, objem, rychlost a rozmanitost. (Ali, et al., 2015)

IoT prostředí získává a shromažďuje data z mnoha senzorů, která jsou následně kategorizována, formulována a využívána k přijímání naprogramovaných rozhodnutí. Generování dat z IoT zařízení může v budoucnu představovat jednu z největších hrozeb. Zařízení jsou navržena tak, aby sloužila ke konkrétnímu účelu než různým aplikacím.

V některých situacích je spíše než použití senzorů pro každou malou aplikaci proveditelné a vhodnější shromažďovat informace logickým úsudkem. (Gupta, et al., 2017)

IoT zařízení neustále přibývá, a to znamená, že i data produkovaná těmito zařízeními dosahují svého maxima. Proto mohou vzniknout problémy se správou nesčetného množství dat a extrahováním požadovaných informací. Největší překážkou, které IoT čelí, je relevance získaných dat s jednáním či chováním uživatele. Takto shromážděná data tedy nemusí být nakonec k ničemu. (Gupta, et al., 2017)

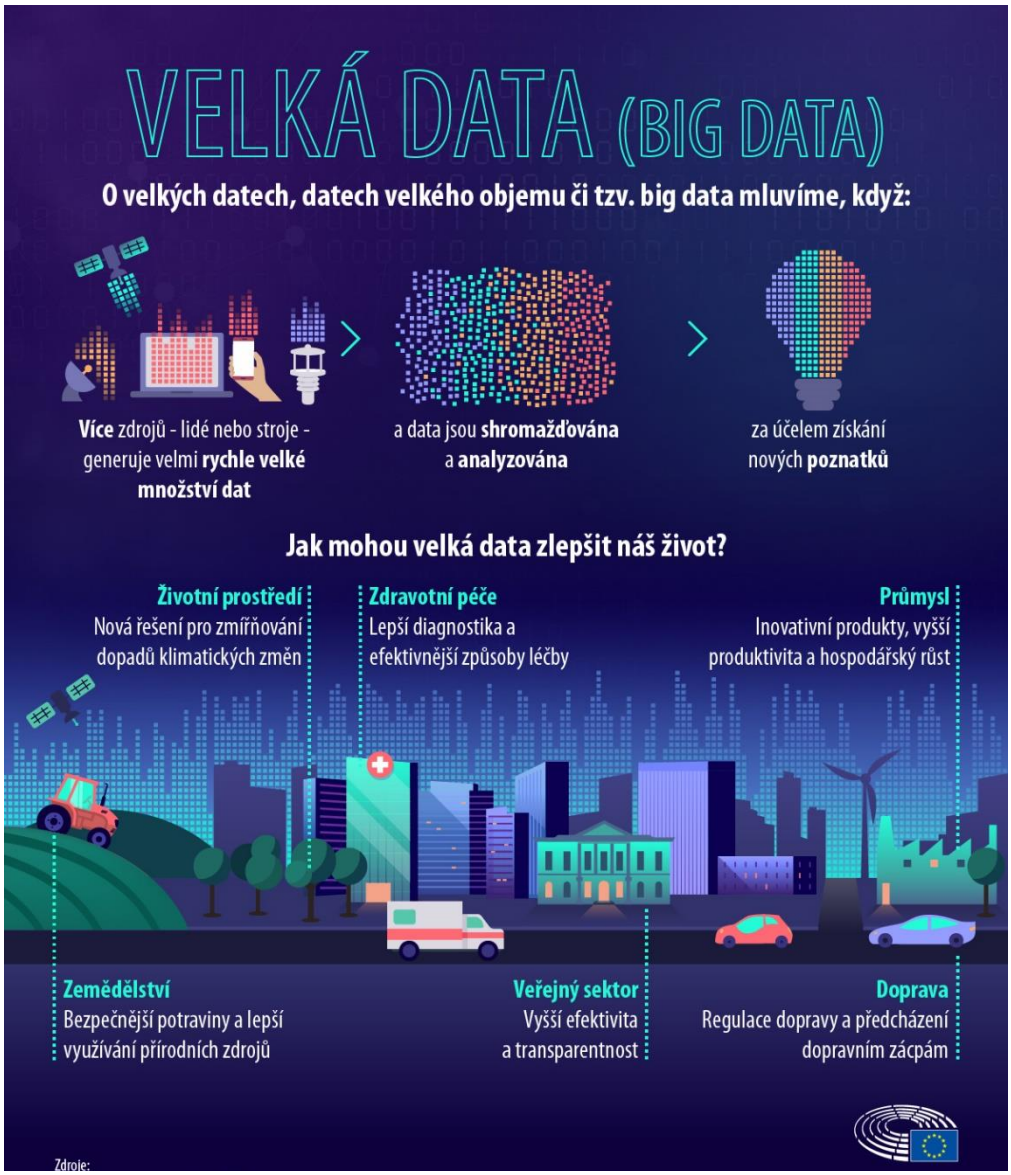
Existují velké rozdíly mezi tradičními databázemi a Big Data řešeními. Tradiční databázové systémy využívají relační design, kde jsou data uložena na základě předem daného schématu a jsou navrženy tak, aby zvládly pracovní zátěž o velikosti terabajtů. Naproti tomu Big Data řešení umožňují ukládat jakýkoliv typ a formát dat včetně nestrukturovaných a polostrukturovaných až o velikost petabajtů. Také nevyžadují žádné předdefinované schéma. (Klein, 2017)

Big Data jsou generována

- Lidmi – v mobilních aplikacích, na webu, včetně sociálních médií a obchodních transakcí, záznamů e-governmentu aj.
- Stroji – shromažďována prostřednictvím senzorů v objektech spojených s internetem věcí jako jsou chytré automobily, továrny, satelity GPS a satelity shromažďujících údaje o počasí atd.

„Data pocházejí z mnoha různých zdrojů. Často jsou stejného typu: například data z GPS z milionů mobilních telefonů se používají ke zmírnění dopravní zácpy; ale může se jednat také o kombinaci různých typů dat. Technologie umožňují, aby data byla shromažďována velmi rychle, téměř v reálném čase, a analyzována pro získání nových poznatků.“ (Evropský parlament, 2023)

„Big Data v průmyslu umožňují společnostem inovovat, a to buď prostřednictvím lepší analýzy potřeb a požadavků lidí, nebo nabídkou zcela nových produktů. Zatímco osobní údaje jsou důležité pro provozování aplikací a platforem, které se staly důležitou součástí jak našeho života, tak ekonomiky, lepší využívání průmyslových údajů by mohlo do EU přinést novou vlnu inovací. Data mohou také zvýšit produktivitu a pomoci snížit náklady, například předvídáním prodeje nebo údržby v továrnách s chytrými systémy.“ viz. Obrázek 3 - Infografika o Big Data (Evropský parlament, 2023)



Obrázek 3 - Infografika o Big Data

3.10 Cloud computing internetu věcí

Jedná se o proces použití hardwaru a softwaru k poskytování služeb prostřednictvím sítě, obvykle internetu. Pomocí této technologie mohou uživatelé přistupovat k souborům a používat aplikace z jakéhokoli zařízení, které má přístup k internetu. (Rashid & Chaturvedi, 2019)

Poskytovatelé cloudových služeb jsou prodejci, kteří poskytují svým zákazníkům prostředky a služby cloud computingu, které jsou dynamicky využívány na základě poptávky zákazníka. (Rashid & Chaturvedi, 2019)

3.10.1 Druhy cloudu

Soukromý cloud, je druh, který se nejlépe funguje pro konkrétní organizaci, kterou je i spravován. (Rashid & Chaturvedi, 2019)

Veřejný cloud je snadno dostupné od poskytovatelů, kteří tento cloud také spravují, poskytují infrastrukturu a služby veřejnosti nebo jakékoli organizace. Zdroje jsou sdílené mezi několika tisíci lidmi. (Rashid & Chaturvedi, 2019)

Komunitní cloud, je druh, kde služby a infrastruktura jsou poskytovány organizacím s podobnými zájmy. (Rashid & Chaturvedi, 2019)

Hybridní cloud je kombinací soukromého a veřejného cloudu, a proto pomáhá při vícenásobném nasazení. (Rashid & Chaturvedi, 2019)

3.10.2 Distribuční modely

IaaS (infrastruktura jako služba)

V tomto modelu poskytovatel cloudových služeb poskytuje sadu virtualizovaných výpočetních zdrojů, jako je procesor, operační paměť, operační systém, aplikační software a uživatelé mohou ty zdroje dynamicky alokovat podle své potřeby. (Rashid & Chaturvedi, 2019)

Mezi výhody tohoto modelu patří snížení výdajů na kapitálové výdaje, uživatelé platí za službu, kterou chtějí a mohou upravovat zdroje na základě svých požadavků a přístup ke zdrojům a infrastruktuře se nachází na podnikové úrovni. (Rashid & Chaturvedi, 2019)

PaaS (platforma jako služba)

V případě PaaS poskytovatel cloudových služeb nabízí, provozuje a udržuje operační systém a další výpočetní zdroje. To zahrnuje i design, vývoj a hostování aplikací, kolaboraci, integraci databází a webových. Nevýhodou PaaS je nedostatečná interoperabilita a portabilita mezi poskytovateli. (Rashid & Chaturvedi, 2019)

Výhodami tohoto modelu jsou kolaborace při vyvíjení aplikací, poskytovatel se stará o veškeré aktualizace, opravy a běžnou údržbu softwaru a vývojářský tým se může soustředit na vývoj aplikace, aniž by se musel starat o testování a nasazení infrastruktury. (Rashid & Chaturvedi, 2019)

SaaS (software jako služba)

V rámci tohoto modelu jsou poskytovatelé cloudových služeb odpovědní za provoz a údržbu aplikačního softwaru, operačního systému a dalších zdrojů. Tento model se uživateli prezentuje jako webové aplikační rozhraní a poskytují se přes něj služby. (Rashid & Chaturvedi, 2019)

SaaS má velmi velkou škálovatelnost, ale jeho největšími výhodami jsou dostupnost z jakékoliv místa s internetovým připojením a eliminace starostí se infrastrukturou. (Rashid & Chaturvedi, 2019)

V modelu SaaS jsou data zákazníka uložena vedle dat ostatních zákazníků v datovém centru poskytovatele SaaS. Poskytovatel cloudu navíc replikuje data na různých místech v různých zemích, aby zajistil jejich dostupnost. V modelu SaaS je za správu bezpečnosti cloudu plně odpovědný poskytovatel. Zdroje poskytované službou SaaS jsou aplikace. Pro vytvoření dokonalého modelu SaaS je třeba důkladně prozkoumat především následující bezpečnostní otázky: Bezpečnost dat, bezpečnost sítě, kolokace dat, integrita dat, segregace dat, řízení přístupu k datům, autentizace a autorizace, důvěrnost dat, bezpečnost webových aplikací, únik dat a zranitelnosti virtualizace. (Abdullayeva, 2023)

3.10.3 Cloud computing a IoT

Cloud Computing a IoT jsou nejoblíbenějším příkladem, který představuje oblast všudypřítomné výpočetní techniky; IoT však není tak populární jako Cloud Computing, oba využívají koncept distribuované výpočetní techniky. Cloud computing je způsob přístupu k velkému množství výpočetních zdrojů a podporuje velký počet uživatelů spolehlivým a decentralizovaným způsobem; je to také levné poskytování softwaru. Cloud computing je

považován za standardní framework pro reprezentaci internetu věcí a jak internet věcí, tak Cloud computing mají řadu výhod a omezení. IoT představuje reálný svět a malé věci, ale kromě tradičních problémů v síti, jako je škálovatelnost a soukromí, má omezené úložiště; na druhé straně cloud computing má prakticky neomezené možnosti a výpočetní výkon. Integrace cloud computingu s IoT se stala velmi důležitým bodem nedávných výzkumů; vytvořit systém schopný překonat mnoho problémů, jako je škálovatelnost, úložné zdroje a virtualizace; za hlavní cíl této integrace lze považovat využití cloud computingu ve výpočetním výkonu, který potřebují senzory a další věci. (Ali, et al., 2015)

3.11 Spotřeba elektrické energie internetu věcí

Otázka spotřeby energie je v bezdrátových sítích kritickým bodem. Efektivita práce senzorů obvykle závisí na životnosti baterie. V dnešní době je většina zařízení vybavena senzory, jako jsou chytré mobilní telefony, tablety a notebooky, které řeší moderní aplikace. Například aplikace předpovědi počasí, která se při určování polohy spoléhá hlavně na GPS; jakmile je aplikace GPS během celého postupu snímání zapnutá, může se baterie velmi rychle vybít. (Ali, et al., 2015)

3.12 Zabezpečení a ochrana soukromí internetu věcí

Cílem bezpečnostních pravidel je ochrana před hrozbami, které se dělí na dva druhy. Vnější hrozby, jako jsou útoky na systém ze strany útočníků, a vnitřní hrozby, které představují zneužití systému nebo informací. Existují tři hlavní faktory bezpečnosti: důvěrnost dat, soukromí a pravdivost. Důvěrnost dat zaručuje přístup k datům a jejich modifikaci pouze oprávněným uživatelům a zahrnuje dva aspekty: zaprvé mechanismus řízení přístupu a zadruhé proces ověřování objektu. Pravdivost je zaručena použitím bezpečnostních pravidel v systému a běžným příkladem pravdivosti jsou digitální certifikáty. Soukromí je definováno jako kontrola přístupu k osobním údajům; a umožňuje zachovat určité informace a údaje v tajnosti; znaky soukromí jsou utajení, anonymita a osamocenost. Většina současných výzkumů usiluje o zvýšení a rozvoj soukromí v aplikacích, technologie pro zvýšení soukromí (Privacy Enhancing Technologies – PET) mohou být orientovány na subjekt, objekt, transakci nebo systém; používají se k ochraně identity na internetu. V

prostředí internetu věcí jsou bezpečnost a soukromí důležité pro zajištění spolehlivé interakce mezi fyzickým a kybernetickým světem. (Ali, et al., 2015)

Správa identit je obor, který se zabývá bezpečností. Zabývá se poskytováním přístupu oprávněným pracovníků, a také kontroluje jejich přístup k různým zdrojům. V současné době se setkáváme s mnoha incidenty, kdy zdroje třetích stran přistupují k neoprávněným datům. Takových incidentů přibývá s objemově rostoucím počtem zařízení, které jsou schopny připojit k internetu. (Gupta, et al., 2017)

Dalším důležitým aspektem je autorizace. Pokud nebude kontrola nad tím, kdo může přistupovat k datům a není reálné, aby každý uživatel měl přístup ke všemu. (Gupta, et al., 2017)

S rozsáhlým spektrem aplikací internetu věcí vzniká otázka bezpečnosti a ochrany soukromí. Bez důvěryhodného a interoperabilního ekosystému pro IoT nemohou nové aplikace dosáhnout vysoké poptávky a mohou ztratit veškerý svůj potenciál. Společně s obecnými bezpečnostními problémy internetu, mobilních sítí a bezdrátových senzorových sítí má IoT také své speciální bezpečnostní výzvy, jako jsou otázky soukromí, autentizační problémy, řízení, ukládání informací a další. viz. Obrázek 4 - Aspekty bezpečnosti mezi IT a IoT (Hassija, et al., 2019)

Obrázek shrnuje různé faktory, kvůli nimž je zajištění bezpečného prostředí IoT mnohem náročnější než u běžných informačních technologií. Kvůli všem těmto problémům a zranitelnostem vytvářejí aplikace IoT úrodnou půdu pro různé druhy kybernetických hrozeb. Po celém světě byly provedeny různé útoky na bezpečnost a soukromí již nasazených aplikací IoT. Zařízení IoT, která jsou nízkonapěťová a méně bezpečná, poskytují bránu pro protivníky, aby vstoupili do domácích a firemních sítí, čímž snadno získávají přístup k uživatelským datům. Navíc se oblast IoT rozšiřuje za hranice pouhých věcí nebo objektů. Byly provedeny různé úspěšné pokusy o implantaci zařízení IoT do lidského těla k monitorování aktuálního stavu různých orgánů. Útočníci mohou cílit na tato zařízení k sledování polohy konkrétní osoby nebo falzifikaci dat. Takový útok se zatím v reálném

životě neodehrál, ale mohl by být extrémně nebezpečný, pokud by byla tato zařízení kompromitována. (Hassija, et al., 2019)

Widespread IT Security	IoT security
Widespread IT has devices which is resource rich	IoT devices need to be carefully provisioned with security measures
Widespread IT is based on resource rich devices	IoT system are composed of devices having limitation in terms of their software and hardware
For wide security and lower capabilities complex algorithm are implemented	only lightweight algorithms are preferred
Homogeneous technology is responsible for high security	IoT with heterogeneous technology produce large amount of heterogeneous data increasing the attack surface

Obrázek 4 - Aspekty bezpečnosti mezi IT a IoT

3.12.1 Bezpečnostní problémy na snímací vrstvě

Bezpečnostní problémy na snímací vrstvě se týkají jednotlivých senzorů a akčních členů. Senzory snímají fyzikální jev, který se děje kolem nich. Na druhé straně akční členy provádějí určitou akci na základě snímaných dat. Hlavní bezpečnostní hrozby, se kterými se lze na snímací vrstvě setkat, jsou následující: (Hassija, et al., 2019)

Zachycení uzlu

IoT aplikace zahrnují několik nízkonapěťových uzlů, což jsou senzory a akční členové. Útočníci mohou zkusit zachytit nebo nahradit uzel škodlivým uzlem. Nový uzel se může jevit jako součást systému, a to může vést o ohrožení celého IoT prostředí. (Hassija, et al., 2019)

Vložení škodlivého kódu

Útočník vloží škodlivý kód do paměti uzlu. Obvykle jsou firmwary a softwary uzlů aktualizovány během provozu, což poskytuje příležitost k vložení kódu. (Hassija, et al., 2019)

Útok vkládání falešných dat

Pokud útočník uzel zachytí, může ho použít k vkládání falešných a chybných dat do IoT systému. To může vést k nesprávným výsledkům a může způsobit nefunkčnost celé aplikace. Útočník může také použít DDoS útok. (Hassija, et al., 2019)

Útok na vedlejší kanál

Kromě přímých útoků na uzly, mohou různé útoky na vedlejší kanál vést k úniku citlivých dat. Mikro-architektury procesorů, elektromagnetické vyzařování a jejich spotřeba energie odhalují protivníkům citlivé informace. Útoky na vedlejší kanál mohou být založeny

na spotřebě energie, laserových útocích, útocích na časování nebo elektromagnetických útocích. Moderní čipy mají na starosti různé protiopatření k prevenci těchto útoků na vedlejší kanál při implementaci kryptografických modulů. (Hassija, et al., 2019)

Odposlech a rušení

IoT aplikace často zahrnují různé uzly nasazené v otevřeném prostředí. V důsledku toho jsou tyto aplikace vystaveny odposlouchávání. Útočníci mohou odposlouchávat a zachytávat data během různých fází provozu, jako je přenos dat nebo ověřování. (Hassija, et al., 2019)

Útok na deprivaci spánku

V takových typech útoků se protivníci snaží vybít baterii nízkonapěťových zařízení na okraji sítě. To vede k odmítnutí služby ze strany uzlů kvůli vybité baterii. To lze provést spuštěním nekonečných cyklů v zařízeních pomocí škodlivého kódu nebo uměle zvyšováním spotřeby energie. (Hassija, et al., 2019)

Útok při bootování

Zařízení jsou zranitelná vůči různým útokům během procesu spouštění. To je způsobeno tím, že vestavěné bezpečnostní procesy nejsou v tomto okamžiku spuštěny, protože tyto zařízení prochází cyklem spánek-bdění. (Hassija, et al., 2019)

3.12.2 Bezpečnostní problémy na síťové vrstvě

Klíčovou funkcí síťové vrstvy je přenos informací získaných ze snímací vrstvy do výpočetní jednotky ke zpracování. (Hassija, et al., 2019)

Útok phishingem

Tyto útoky se často týkají situace, kdy je minimálním úsilím útočníka cíleno na několik IoT zařízení. Útočníci očekávají, že alespoň několik zařízení se stane obětí útoku. Existuje možnost setkání se s phishingovými stránkami při návštěvě uživatelů webových stránek na internetu. Jakmile je kompromitován účet uživatele, stává se celé prostředí IoT zranitelným vůči kybernetickým útokům. Síťová vrstva v IoT je silně zranitelná vůči útokům phishingových stránek. (Hassija, et al., 2019)

Útok na přístup

Útok na přístup je také označován jako pokročilá trvalá hrozba „advanced persistent threat“. Jedná se o typ útoku, při kterém neoprávněná osoba nebo útočník získá přístup k síti IoT. Útočník může zůstat v síti nepozorován po dlouhou dobu. Účelem tohoto druhu útoku

je krádež cenných dat nebo informací spíše než způsobení škody síti. Aplikace IoT neustále přijímají a přenášejí cenná data a jsou proto vysoko zranitelné vůči takovýmto útokům. (Hassija, et al., 2019)

DDoS/DoS útok

Při takových útocích útočník zaplavuje cílové servery velkým množstvím nežádoucích požadavků. To způsobuje vyřazení cílového serveru a tím narušení služeb pro skutečné uživatele. Pokud jsou k napadení cílového serveru použity různé zdroje, pak je takový útok označován jako DDoS nebo distribuovaný útok odmítnutí služby. Tyto útoky nejsou specifické pro aplikace IoT, ale kvůli heterogenitě a složitosti sítí IoT je síťová vrstva náchylná k takovým útokům. Mnoho zařízení v aplikacích IoT není pevně konfigurováno, a proto se stávají snadnými branami, skrze které mohou útočníci spustit DDoS útoky na cílové servery. (Hassija, et al., 2019)

Útok na přenos dat

Aplikace IoT se zabývají velkým množstvím ukládání a výměny dat. Data jsou cenná a jsou proto vždy cílem hackerů a dalších protivníků. Data uložená na lokálních serverech nebo v cloudu mají bezpečnostní riziko, ale data, která jsou v pohybu nebo se pohybují z jednoho místa na druhé, jsou ještě více zranitelná vůči kybernetickým útokům. V IoT aplikacích dochází k mnoha pohybům dat mezi senzory, akční členy, cloudu atd. Při těchto pohybech dat se používají různé technologie připojení, a proto jsou aplikace IoT náchylné k narušení dat. (Hassija, et al., 2019)

Útok na směrování

Při těchto útocích mohou napadané uzly v IoT aplikaci zkoušet přesměrovat trasy směrování během přenosu dat. Útoky na směrování jsou konkrétním typem útoku, při kterém protivník propaguje uměle nejkratší cestu směrování a přitahuje uzly, aby směrovaly provoz skrze ni. (Hassija, et al., 2019)

3.12.3 Bezpečnostní problémy na middleware vrstvě

Úkolem middleware vrstvy je vytvořit abstrakní vrstvu mezi síťovou a aplikační vrstvou. (Hassija, et al., 2019)

Útok „SQL Injection“

Middleware vrstava je náchylná k útokům SQL Injection. Při takových útocích může útočník vložit škodlivé SQL příkazy do programu, poté mohou útočníci získat soukromá data jakéhokoli uživatele, a dokonce mohou měnit záznamy v databázi. (Hassija, et al., 2019)

Útok „Signature Wrapping“

Ve webových službách používaných v middleware se používají XML podpisy. Při útoku útočník prolomí algoritmus podpisu a může provádět operace nebo upravovat odposlouchanou zprávu prostřednictvím zneužití zranitelností v protokolu SOAP (Simple Object Access Protocol) (Hassija, et al., 2019)

„Malware Injection“ do cloudu

Při napadení cloudu malwarem může útočník získat kontrolu, vložit škodlivý kód nebo může vložit virtuální stroj do cloudu. Útočník se vydává za platnou službu tím, že se snaží vytvořit instanci virtuálního stroje nebo škodlivého modulu služby. Tímto způsobem může útočník získat přístup k žádostem o službu oběti a zachytávat citlivá data, která mohou být upravena podle konkrétní situace. (Hassija, et al., 2019)

„Flooding Attack“ do cloudu

Tento útok funguje téměř stejně jako útok DoS v cloudu a ovlivňuje kvalitu služby. Pro vyčerpání zdrojů cloudu útočníci neustále odesílají více žádostí na službu. Tyto útoky mohou mít velký dopad na cloudové systémy zvyšováním zátěže na cloudové servery. (Hassija, et al., 2019)

3.12.4 Bezpečnostní problémy na aplikační vrstvě

Aplikační vrstva se přímo zabývá a poskytuje služby koncovým uživatelům. Tato vrstva má své specifické bezpečnostní problémy, které se nevyskytují na jiných vrstvách. Mnoho aplikací IoT se také skládá z podvrstvy mezi síťovou vrstvou a aplikační vrstvou, která se obvykle nazývá vrstva podpory aplikací. Vrstva podpory podporuje různé obchodní služby a pomáhá při inteligentní alokaci zdrojů a výpočtech. (Hassija, et al., 2019)

Krádež dat

IoT Aplikace zpracovávají mnoho kritických a privátních dat. Uživatelé budou váhaví registrovat svá privátní data v aplikacích, pokud jsou tyto aplikace náchylné k útokům na krádeže dat. Šifrování dat, izolace dat, autentizace uživatele a sítě, správa soukromí atd. jsou některé z technik a protokolů používaných k zabezpečení aplikací proti krádežím dat. (Hassija, et al., 2019)

Útok na kontrolu přístupu

Kontrola přístupu je mechanismus autorizace, který umožňuje přístup k datům nebo účtu pouze legitimním uživatelům nebo procesům. Útok na kontrolu přístupu je kritickým útokem v aplikacích, protože jakmile je přístup ohrožen, stává se celá IoT aplikace zranitelnou vůči útokům. (Hassija, et al., 2019)

Útok na přerušení služby

Tyto útoky brání legitimním uživatelům využívat služby aplikací IoT tím, že uměle zaneprázdní servery nebo síť tak, aby nebyly schopny reagovat. (Hassija, et al., 2019)

Útok vkládáním škodlivého kódu

Pokud je systém zranitelný vůči škodlivým skriptům a odchylkám způsobeným nedostatečnou kontrolou kódu, pak by to byl první vstupní bod, který by útočník zvolil. Obvykle útočníci používají „cross-site scripting“ k vložení nějakého škodlivého skriptu do jinak důvěryhodné webové stránky. Úspěšný útok může vést k ovládnutí účtu IoT a paralyzování celého IoT systému. (Hassija, et al., 2019)

3.13 Metoda AHP

Analytický hierarchický proces je metoda vytvořena americkým profesorem T.L. Saatym. Provádí se pro přípravu rozhodnutích při složitých rozhodovacích situací a také napomáhá usnadnit a zrychlit přirozený proces rozhodování. (Šubrt, et al., 2011)

Analytický hierarchický proces používaný ve vícekriteriálním rozhodování vychází ze stanovení kritérií mezi jednotlivými faktory, které ovlivňují rozhodování. Pokud se rozhodovatel rozhoduje mezi více variantami, je pro každou variantu nutné stanovit kritéria a k těmto kritériím stanovit preferenci. Získání co nejvíce pravděpodobných hodnot kritérií je nejtěžší částí rozhodovacího procesu. (Tomeš, 2019)

AHP se používá v mnoho odvětvích průmyslu pro vyřešení problémů s rozhodováním podle různých kritérií, které zahrnují subjektivní mínění. Nicméně, AHP je často kritizována za její neschopnost adekvátně se přizpůsobit přirozené nejistotě a nepřesnosti spojené s mapováním rozhodovacích preferencí na přesné číslo. (Tomeš, 2019)

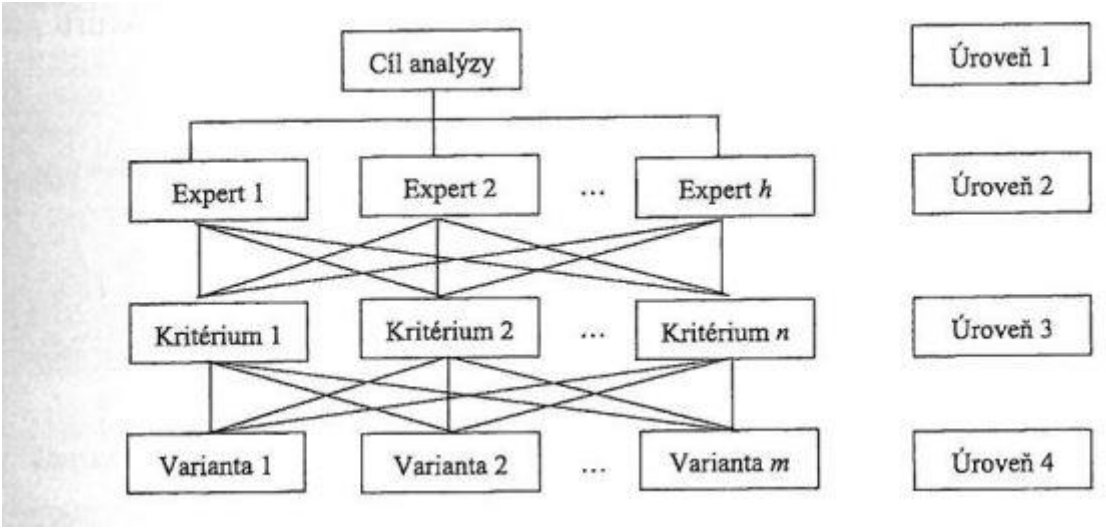
3.13.1 Postup

Definice rozhodovacího modelu

- Zde se definuje konkrétní problém a stanoví cíl rozhodování.
- Také se sestaví soubor kritérií a provede výběr alternativ.
- Nastaví se aspirační úrovně pro konkrétní kritéria, tzn. minimální a maximální limit pro všechna kritéria.

Vytvoření hierarchického struktury procesu

- Do stromového struktury se transformují jednotlivé části AHP.
- Na nejvyšší úrovni je cíl konkrétního rozhodování.
- Na meziúrovních se nachází jednotlivá kritéria.
- Nejnižší úroveň představuje jednotlivé varianty.



Obrázek 5 - hierarchická struktura procesu

Stanovení vah kritérií

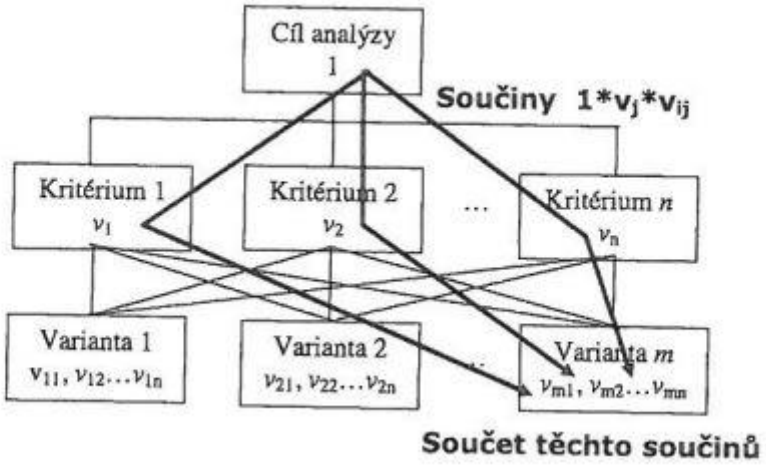
- Pro každou dvojici kritérií se vytvoří matice porovnání, kde se stanoví relativní preference vůči sobě. Používá se Saatyho stupnice pro kvantifikaci preferencí.
- V některých případech se dá použít mezihodnoty: 2,4,6,8.

Stupeň hodnocení	Význam preference kritérií
1	Rovnocenná kritéria
3	Slabě preferované
5	Silně preferované
7	Velmi silně preferované
9	Absolutně preferované

Tabulka 1 - Saatyho stupnice

Stanovení kompromisní varianty

- Pro každou variantu se sestaví vážená dílčí váha na základě vah a preferencí kritérií.
- Syntézou preferencí se určí kompromisní (optimální) varianta.



Obrázek 6 - Syntéza preferencí

4 Vlastní práce

Obsahem praktické části bude výběr nástrojů pro správu IoT zařízení a jejich následné zhodnocení podle stanovených kritérií. Výběr nástrojů a kritérií se stanovil z poznatků v teoretické části. Pro zhodnocení těchto nástrojů byla vybrána metoda AHP, jejíž charakterizace a postup řešení je uveden v kapitole 3.13.1.

4.1 Výběr nástrojů pro správu IoT zařízení

AWS IoT Core

Byl zahrnut pro svou škálovatelnost a širokou podporu, což zajišťuje efektivní správu velkého množství IoT zařízení.

Microsoft Azure IoT Hub

Byl zvolen pro svou integraci s rozsáhlým ekosystémem Microsoftu a vysoké bezpečnostní standardy, což poskytuje robustní infrastrukturu pro správu připojených zařízení.

Particle

Byl zařazen do výběru díky své orientaci na rychlost a jednoduchost implementace, což je klíčové pro projekty s omezenými zdroji.

Losant IoT Platform

Byl vybrán do výběru pro své vizuální programování a flexibilitu, což umožňuje tvorbu přizpůsobených řešení pro úplné začátečníky.

4.2 Vymezení požadavků (kritérií) nástrojů pro správu IoT zařízení

Bezpečnost

Vyžadujeme ochranu před hrozbami specifikované v kapitole 3.12 a také pravidelnou aktualizace zabezpečovacích systémů.

Škálovatelnost

Definujeme konkrétní limity pro škálovatelnost, jako maximální počet připojených zařízení, a stanovujeme požadavky na odezvu v případě zvýšeného provozu. Toto kritérium bylo vybráno na základě informací popsaných v kapitole 3.7.

Monitoring

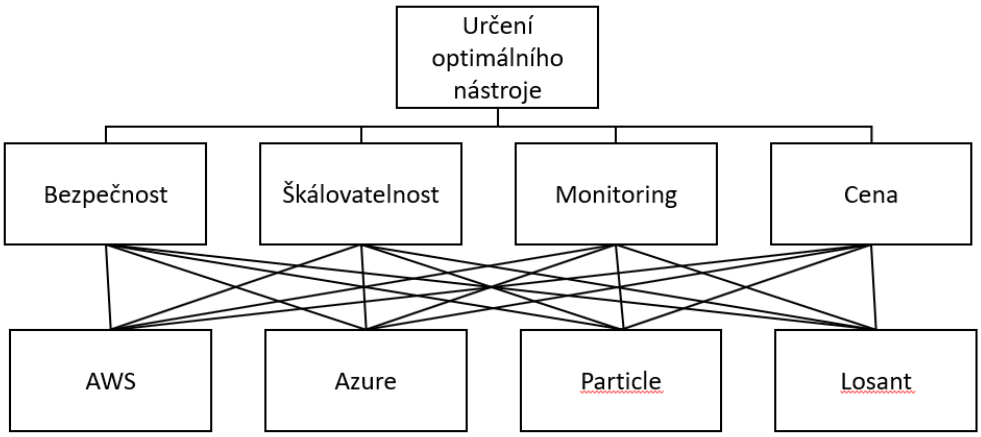
Stanovujeme požadavky na detailní záznamy monitorovacích dat a diagnostických informací. Požadujeme schopnost vzdálené diagnostiky a monitorování a ukládání Big Data. Tento koncept byl popsán v kapitole 3.9.

Cena

Hodnocena bude podle počátečních výdajů, ale také provozních výdajů a další poplatky spojeny s používáním daného nástroje. Cena byla zahrnuta na základě nutnosti pro zprovoznění IoT prostředí.

4.3 Aplikace AHP pro zhodnocení nástrojů

Podle postupu v 3.13.1 byla zhotovena hierarchická struktura AHP, která obsahuje jednotlivé IoT nástroje a také kritéria podle kterých budou hodnocena mezi sebou.



Obrázek 7 - Hierarchická struktura AHP, vlastní zpracování

4.4 Stanovení vah kritérií

V následující tabulce stanovení vah kritérií byly mezi sebou zhodnoceny jednotlivá kritéria pro výběr nástroje pro správu IoT zařízení. Nejsilněji preferovaným kritériem byla Bezpečnost oproti ostatním kritériím. Nejdůležitějším údajem je pro další postup sloupec „Váha“, který udává jednotlivé váhy kritérií. viz. Tabulka 2

	Bezpečnost	**Škálovatelnost**	**Monitoring**	**Cena**	**Geo. p.**	**Váha**
Bezpečnost	1	7	9	5	4,213	0,674
Škálovatelnost	0,14	1	3	2	0,962	0,154
Monitoring	0,11	0,33	1	0,33	0,333	0,053
Cena	0,2	0,5	3	1	0,74	0,118
Součet					6,248	1

Tabulka 2 - Stanovení vah kritérií pomocí Saatyho stupnicí

4.5 Stanovení kompromisního řešení

V následujících tabulkách jsou porovnány jednotlivé nástroje pro správu IoT zařízení. Každá konkrétní tabulka porovnává nástroje vždy jen pro jedno konkrétní kritérium. Nejdůležitějším údajem v těchto tabulkách je hodnoty ve sloupci Vážena váha, která je spočtena součinem Váhy nástrojů a Váhy konkrétního kritéria, nacházející se v levém rohu, každé tabulky , které bylo vypočteno v předchozí tabulce. viz. Tabulka 2

4.5.1 Bezpečnost

Nástroje pro správu IoT zařízení byly zde hodnoceny podle kritéria Bezpečnost.

0,674	**AWS**	**Azure**	**Particle**	**Losant**	**Geo. p.**	**Váha**	**Vážená váha**
AWS	1	1	5	7	2,432	0,424	0,286
Azure	1	1	5	7	0,962	0,424	0,286
Particle	0,2	0,2	1	3	0,333	0,103	0,069
Losant	0,14	0,14	0,33	1	0,74	0,05	0,034
Součet					6,248	1	0,674

Tabulka 3 - Saatyho matice pro kritérium Bezpečnost

4.5.2 Škálovatelnost

Nástroje pro správu IoT zařízení byly zde hodnoceny podle kritéria Škálovatelnost.

0,154	**AWS**	**Azure**	**Particle**	**Losant**	**Geo. p.**	**Váha**	**Vážená váha**
AWS	1	3	5	5	2,943	0,558	0,086
Azure	0,33	1	3	3	1,316	0,249	0,038
Particle	0,2	0,33	1	1	0,508	0,096	0,015
Losant	0,2	0,33	1	1	0,508	0,096	0,015
Součet					5,275	1	0,154

Tabulka 4 - Saatyho matice pro kritérium Škálovatelnost

4.5.3 Monitoring

Nástroje pro správu IoT zařízení byly zde hodnoceny podle kritéria Monitoring.

0,053	**AWS**	**Azure**	**Particle**	**Losant**	**Geo. p.**	**Váha**	**Vážená váha**
AWS	1	3	0,33	0,2	0,669	0,118	0,006
Azure	0,33	1	0,2	0,14	0,312	0,055	0,003
Particle	3	5	1	0,33	1,495	0,263	0,014
Losant	5	7	3	1	3,201	0,564	0,03
Součet					5,678	1	0,053

Tabulka 5 - Saatyho matice pro kritérium Monitoring

4.5.4 Cena

Nástroje pro správu IoT zařízení byly zde hodnoceny podle kritéria Cena.

0,118	**AWS**	**Azure**	**Particle**	**Losant**	**Geo. p.**	**Váha**	**Vážená váha**
AWS	1	3	0,14	0,2	0,541	0,089	0,0106
Azure	0,33	1	0,11	0,17	0,27	0,044	0,0053
Particle	7	9	1	0,5	2,369	0,39	0,0462
Losant	5	7	2	1	2,893	0,476	0,0564
Součet					6,072	1	0,118

Tabulka 6 - Saatyho matice pro kritérium Cena

5 Výsledky a diskuse

5.1 Výsledky

Pomocí AHP metodou byly metodicky zhodnoceny čtyři platformy pro správu IoT zařízení, AWS IoT Core, Microsoft Azure, Particle a Losant. Platformy byly hodnoceny na základě čtyř kritérií, Bezpečnost, Škálovatelnost, Monitoring a Cena. Výsledek by měl ukázat optimální kompromisní variantu.

Nástroj	**Syntéza preferencí**	**Pořadí**
AWS	0,388	1.
Azure	0,332	2.
Particle	0,144	3.
Losant	0,135	4.

Tabulka 7 - Syntéza preferencí

5.2 Diskuse výsledku

Výsledek zpracovaný přes AHP metodu ukázal AWS IoT Core jako optimální platformu pro správu IoT zařízení. Důvodem proč AWS IoT Core vyšel jako optimální výsledek bylo omezený výběr kritérií a variant (platforem). To ovšem neznamená, že jsou ostatní platformy nepoužitelné.

5.3 Diskuse o budoucnosti IoT platforem

Integrace „Building Information Modelling“ s daty z IoT zařízení představuje výkonné schéma pro aplikace ke zlepšení efektivity provozu. Výzkum integrace BIM a IoT je však stále v počáteční fázi, je třeba porozumět současné situaci v oblasti integrace BIM a zařízení IoT. (Tang, et al., 2019)

Aby bylo možné provádět analýzu velkých dat v reálném čase, je třeba získané informace ukládat do online úložiště, ke kterému lze přistupovat z více zařízení IoT. Návrhové vzory, jako je aktualizace v cloudu založená na zprávách a aktualizace v cloudu na vyžádání pro SOA, mohou účinně řešit problém cloudového úložiště informací BIM a více zařízení IoT a dotazování na informace. Webové služby a cloudové služby je třeba kombinovat, aby bylo možné provádět efektivní správu a zpracování dat. (Tang, et al., 2019)

Nedostatek standardů je považován za otevřený problém pro paradigma internetu věcí a cloudu. Ačkoli se některé výzkumy snažily standardizovat paradigmata IoT a cloud, neexistují jasné standardní protokoly, architektura a rozhraní API, které by propojovaly různá zařízení a služby IoT v cloudu. Jako budoucí směr výzkumu je třeba vytvořit obecný standard pro propojení hardwaru, dat BIM, komunikačních protokolů, ontologií, sémantických pravidel, middlewaru a aplikací. (Tang, et al., 2019)

6 Závěr

Teoretická část BP byla zaměřena na zjištění aktuálního stavu poznání dané problematiky. Byla provedena analýza literárních zdrojů v oblasti problematiky správy IoT zařízení. Z této analýzy bylo zjištěno, které aspekty jsou kritické pro správu IoT zařízení. Dále byla popsána metoda AHP, která je využívána v praktické části pro zhodnocení platforem.

V prvním kroku praktické části byly vybrány nástroje AWS IoT Core, Microsoft Azure, Particle a Losant IoT platform na základě, zda splňují aspekty popsané v teoretické části.

V následném korku byly stanoveny kritéria byla charakterizována v teoretické části a jejich výběr vycházel z analýz z literárních zdrojů.

Ve třetím korku práce byly stanoveny váhy. Silněji byly preferované kritéria Bezpečnost a Škálovatelnost.

Dalším krokem bylo provedení metody AHP.

Z výsledků vyplývá že nástroj AWS IoT Core je vhodný velké projekty, které požadují, aby byla bezpečnost dat na prvním místě.

Microsoft Azure je velmi škálovatelný z důvodu, že existuje v ekosystému Microsoftu.

Particle nabízí cenově dostupné plány pro menší projetky.

Losant IoT platform nabízí cenu podle potřeb zákazníka.

Internet věcí je technologie, která se každý mění, je těžké určit, zda AWS IoT Core, který v této práci vyšel jako nejlepší variantu, bude vůbec relevantní v budoucnu.

7 Seznam použitých zdrojů

Abdullayeva, F., 2023. Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results in Control and Optimization*, Září, Svazek 12, p. 100268.

Ali, Z. H., Ali, H. A. & Badawy, M. M., 2015. Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions. *International Journal of Computer Applications*, říjen, pp. 975-8887.

Evropský parlament, 2023. *Velká data (big data): definice, výhody a výzvy (infografika)*, Štrasburk: autor neznámý

Gupta, A., Christie, R. & Manjula, R., 2017. Scalability in Internet of Things: Features, Techniques and Research Challenges. *International Journal of Computational Intelligence Research*, 13(7), pp. 1617-1627.

Hassija, V. a další, 2019. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access*, pp. 82721-82743.

IBM, 2021. *What is virtualization?*. [Online] Available at: https://www.ibm.com/topics/virtualization [Přístup získán 13 Březen 2024].

Klein, S., 2017. *IoT Solutions in Microsoft's Azure IoT Suite: Data Acquisition and Analysis in the Real World.* Berkeley: Apress.

Madakam, S., Ramaswamy, R. & Tripathi, S., 2015. Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, 2015, 3(5), pp. 164-173.

Rashid, A. & Chaturvedi, A., 2019. Cloud Computing Characteristics and Services: A Brief Review. *International Journal of Computer Sciences and Engineering*, 28 Únor, 7(2).

Rossman, J., 2016. *The Amazon Way on IoT: 10 Principles for Every Leader from the World's Leading Internet of Things Strategies.* 1. editor Bellevue: Clyde Hill Publishing.

Šubrt, T. a další, 2011. *Ekonomicko-matematické metody.* Plzeň: Aleš Čeně.

Tamboli, A., 2022. *Build Your Own IoT Platform.* 2 editor Sydney: Apress.

Tang, S. a další, 2019. A review of building information modeling (BIM) and the internet of things (IoT) devices integration: Present status and future trends. *Automation in Construction*, Květen, Svazek 101, pp. 127-139.

Tomeš, R., 2019. Metoda na zvýšení konzistence matice párových. *Journal of Global Science*.

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam použitých zkratek

IoT – internet of things, internet věcí
SOA – service oriented architecture, architektura orientovaná služba
API – application programming interface, aplikační programové prostředí
BIM – Building Information Modelling
AHP – analytický hierarchický proces