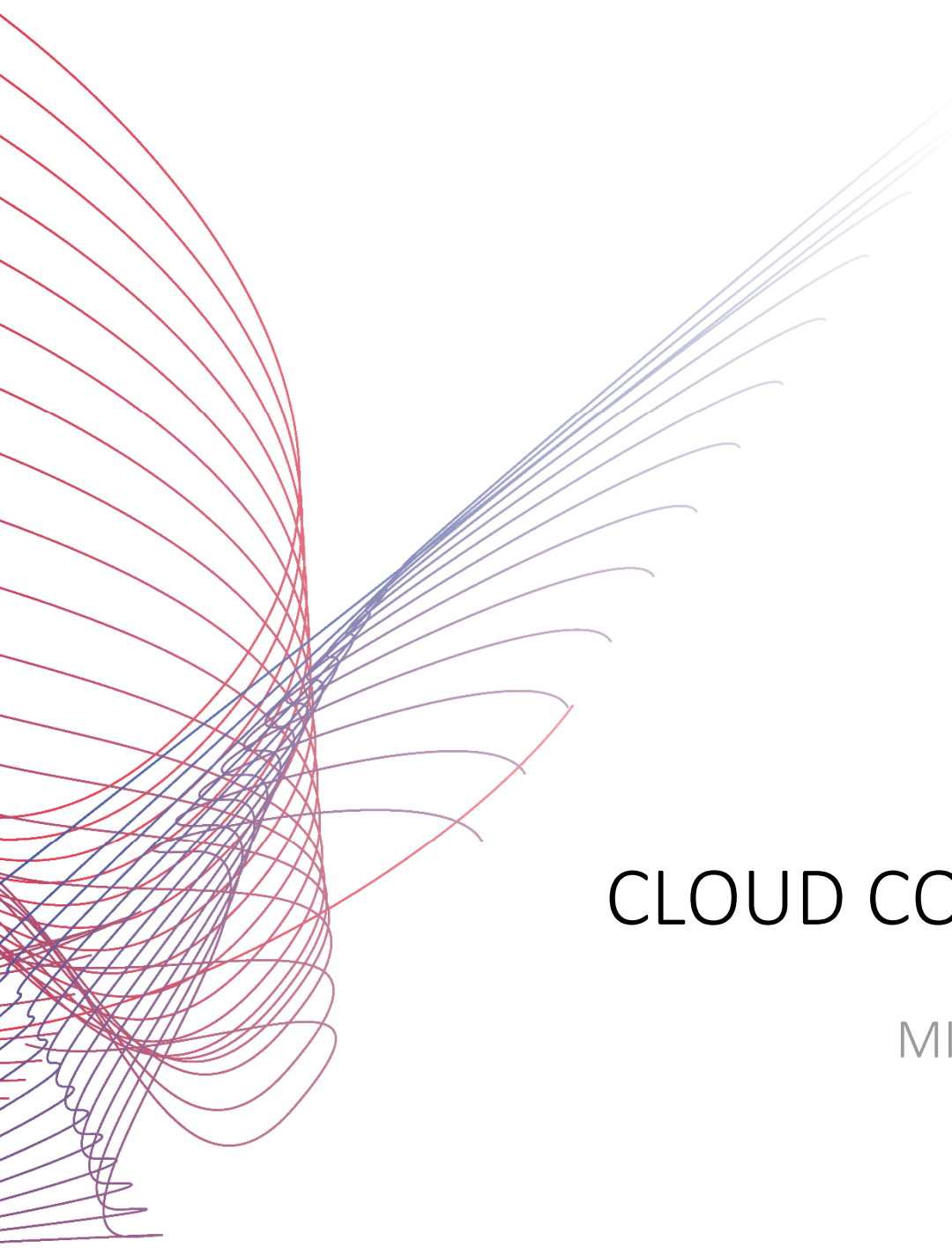




TECH pedia



CLOUD COMPUTING

MIGUEL SORIANO

Název díla: Cloud computing
Autor: Miguel Soriano
Přeložil: Pavel Bezpalec
Vydalo: České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktní adresa: Technická 2, Praha 6
Tel.: +420 224352084
Tisk: (pouze elektronicky)
Počet stran: 31
Edice (vydání): 1. vydání, 2017
ISBN 978-80-01-06211-1

TechPedia

European Virtual Learning Platform for
Electrical and Information Engineering

<http://www.techpedia.eu>

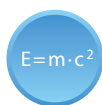


Tento projekt byl realizován za finanční podpory
Evropské unie.

Za obsah publikací odpovídá výlučně autor.

Publikace (sdělení) nereprezentují názory Evropské
komise a Evropská komise neodpovídá za použití
informací, jež jsou jejich obsahem.

VYSVĚTLIVKY



Definice



Zajímavost



Poznámka



Příklad



Shrnutí



Výhody



Nevýhody

ANOTACE

Tento modul obsahuje některé důležité informace pro základní orientaci studentů v oblasti cloud computingu. Obsahuje přehled historie této technologie, architekturu, služby a modely nasazení. Dále jsou též diskutovány výhody a nevýhody cloud computingu oproti předchozí architektuře.

CÍLE

Tento modul poskytuje základní informace o cloud computingu. Cloud computing je jedním z horkých trendů v technologiích. Tento modul pomáhá objasnit význam, různé modely a možnosti nabízené touto technologií. Tento dokument se snaží objasnit dostupné spektrum nabídek a terminologii použitou na jejich popis v oblasti cloud computingu.

Hlavním cílem tohoto modulu je, aby čtenář dovedl určit, zda typ nabízeného řešení může být pro organizaci užitečný, jaká služba a model nasazení je nejvýhodnější pro uspokojení všech požadavků organizace. Čtenář pak bude schopen identifikovat veškeré výhody a hlavní rizika použití cloud computingu.

LITERATURA

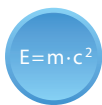
- [1] U.S. National Institute of Standards and Technology (NIST) The NIST Definition of Cloud Computing. <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>. Sept. 2011. <http://www.nist.gov/itl/cloud>
- [2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia “Above the Clouds: A Berkeley View of Cloud Computing” University of California at Berkeley. <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS>
- [3] Cary Landis, Dan Blacharski *Cloud Computing Made Easy: An Easy to Understand Reference About Cloud Computing*. Virtual Global Inc, 2013, ISBN 978-1482779424
- [4] Douglas F. Parkhill *The Challenge of the Computer Utility*. Addison-Wesley Publishing Company, (1966), ASIN: B000O121OS, ISBN : 0240507177
- [5] Antonio Regalado, Who coined “Cloud Computing”? MIT Technology Review, USE, Oct. 2011
- [6] M. N.O. Sediku, S. M. Muse, O.D. Momoh “Cloud computing: Opportunities and challenges” IEEE Potentials 02/2014; 33(1):34-36
- [7] Jinesh Varia *Architecting for the Cloud: Best Practices* January 2010

- [8] Peter Mell, Tim Grance “Effectively and Securely Using the Cloud Computing Paradigm”
- [9] Eugene Gorelik *Cloud Computing Models*, January 2013
- [10] The cloud tutorial <http://thecloudtutorial.com>
- [11] D. Catteddu and G. Hogben, “Cloud Computing: Benefits, Risks and Recommendations for Information Security,” ENISE, 2009;
www.enise.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport
[\[http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport\]](http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport).
- [12] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,” <http://www.cloudsecurityalliance.org/cseguide.pdf>.

Obsah

1	Úvod. Co je cloud computing.....	7
2	Historie.....	9
3	Vlastnosti cloud computingu.....	12
4	Komponenty a architektura cloud computingu	14
5	Servisní modely cloud computingu.....	16
5.1	Software as a Service	17
5.2	Platform as a Service.....	18
5.3	Infrastructure as a Service	20
6	Modely nasazení	22
6.1	Veřejný cloud	23
6.2	Privátní cloud	24
6.3	Komunitní cloud.....	25
6.4	Hybridní cloud.....	26
7	Použití a aplikace.....	27
8	Výhody a nevýhody cloud computingu	28
9	Bezpečnost v cloudu. Možná rizika	30
10	Závěr.....	31

1 Úvod. Co je cloud computing.



Podle NIST je cloud computing model navržený pro umožnění pohodlného přístupu ke sdíleným konfigurovatelným výpočetním zdrojům (sítím, serverům, úložištím, aplikacím, službám), které mohou být okamžitě poskytnuty s minimální správou nebo potřebou zásahu poskytovatele této služby [1].

Autoři doplňující definice z RAD Lab z univerzity v Berkeley [2] považují cloud computing jak za aplikace dodávané jako služby prostřednictvím internetu tak též i za hardware a systémový software v datových centrech, které poskytují tyto služby.

Cloud computing je v podstatě distribuovaná výpočetní platforma, která poskytuje svoje prostředky širokému spektru uživatelů na škálování, virtualizaci hardwarové a/nebo softwarové infrastruktury přes internet.

Cloud computing dovoluje sdílet své výpočetní zdroje přes Internet. Sestává ze souboru technologií, které nabízí poskytovatel ve formě služeb samotným zákazníkům, jako například skladovací prostor, výpočetní výkon za použití hardwarové/ softwarové distribuované virtualizované sítě. Poskytovatel takovýchto služeb může vlastnit nebo hostovat hardware nebo software potřebný pro běh různých privátních nebo obchodních aplikací.

Cloud computing je komplexní a rychle se rozvíjející koncept. Cloud computing může být považován za distribuovaný systém, který nabízí výpočetní výkon přes počítačovou komunikační síť, obvykle přes Internet. Zdroje v cloudu jsou jasně definované pro uživatele a uživatel nepotřebuje vědět, kde přesně se tyto zdroje nacházejí. Ty mohou být sdílené mezi větším počtem uživatelů, kteří jsou schopni přistupovat k aplikacím a datům kdykoli a odkudkoli. Jednoduchým příkladem cloud computingu je email. Poskytovatel emailové služby spravuje server a poskytuje k němu přístup. Uživatel jednoduše zadá jen adresu do prohlížeče a zadá uživatelské údaje pro přihlášení. Software na úložišti není na jeho osobním počítači, ale existuje jako služba v cloudu.

Hlavním cílem cloud computingu je vytvoření lepšího využití distribuovaných zdrojů a řešení problémy rozsáhlých výpočtů. Slovo „cloud - mrak“ je metafora, která znázorňuje web jako prostor, ve kterém jsou výpočetní zdroje předinstalované a existují jako služba [1]. Operační systém, aplikace, skladovací prostor, data a kapacita zpracování dat, všechno existuje jako webová služba, která je připravená ke sdílení mezi uživateli.

Používání cloudových služeb má za následek výhody využívání velkého množství výpočetního výkonu nebo diskového prostoru, který je zároveň poskytován jako internetová služba. Není potřeba fyzicky vlastnit servery v rámci korporátní sítě, stačí mít osobní počítač a software. Obecně jsou tyto služby poskytovány transparentním způsobem, platforma skrývá složitost infrastruktury cloudu před uživateli a aplikacemi.



V cloud computingu jsou modely, výpočetní výkon, software, úložiště a platformy na vyžádání poskytovány zákazníkům přes Internet. Všechny typy aplikací od

textových editorů po vysoce sofistikovaný software může pracovat v cloudu. Přístup, který tato technologie poskytuje k zdrojům a službám, může být zvětšován nebo zmenšován podle požadavků. Za cloud computing se účtuje poplatek podle množství využívaných zdrojů.

Zatímco výhod cloud computingu je mnoho, nevýhod také není málo. Jestliže je cloud computing vhodně použitý, je vhodný pro každý typ podnikání.



Hlavními výhodami cloud computingu jsou samoobslužné služby na vyžádání, všude přítomný přístup k síti, sdružování zdrojů nezávisle na umístění a přenos rizika. Přidané výhody jsou nízké pořizovací náklady, kvalita služby, jednoduchá správa, kvalita služeb, spolehlivost, žádné velké investice do infrastruktury, lepší přizpůsobení a škálovatelnost a lepší správa.



V dnešní době jsou největšími výzvami cloud computingu soukromí a bezpečnost. Nevýhodami jsou nedostatečná nebo limitovaná kontrola, přímá závislost na poskytovateli, která je známá jako „vendor lock-in“. Je těžké migrovat technologii od jednoho poskytovatele k druhému.



Vivek Kundra, federální CIO a kdysi technologický ředitel District of Columbia řekl: „Cloud bude dělat pro vládu to, co Internet v devadesátých letech.“ [3]

2 Historie

Informační technologie byly vždy považovány za hlavní kámen úrazu velkých organizací z pohledu nákladů a správy. Ačkoli získal informační průmysl mnoho zkušeností a v posledním desetiletí se výrazně posunul, faktory jako komoditizace hardware, open-source software, virtualizace, globalizace, pracovní síly a agilní IT procesy podporovaly vývoj nových technologií a obchodních modelů.



Cloud computing je přirozenou evolucí všeobecně adaptované virtualizace, architektur orientovaných na služby a autonomního výpočetního modelu. V skutečnosti je cloud computing novým výrazem pro dlouho udržovaný sen computingu jako prospěšného nástroje, který se do komerční reality propracoval před nedávnem. Tato evoluce začala v 50. letech, kdy bylo umožněno přistupovat více uživatelům k centrálnímu počítači přes velmi limitované terminály. Později v 70. letech byl vytvořen koncept virtuálních strojů. Vývoj cloud computingu měl spád v 90. letech, kdy Internet začal poskytovat značné šířky pásma, a telekomunikační společnosti začaly nabízet virtualizované privátní sítě.

Někteří experti připisují koncept cloudu Johnovi McCarthy, profesorovi na Univerzitě Stanford a zakladateli programovacího jazyka Lisp, který v roce 1961 navrhl myšlenku výpočetního výkonu, která by byla veřejně doručitelná a byla by podobná principům veřejného výpočetního střediska.

V roce vydal 1966 Douglas F. Parkhill knihu „The Challenge of the Computer Utility“ [4], která obsahovala vizi budoucího computingu, předpovídaje, že počítačový průmysl bude podobný veřejné službě, "která přes komunikační linky připojí mnoho vzdálených uživatelů do centrálního počítačového zařízení". V knize je uvedeno několik charakteristik cloud computingu (pružné poskytování, online, dodávka jako služba, iluze/pocit neomezeného množství).

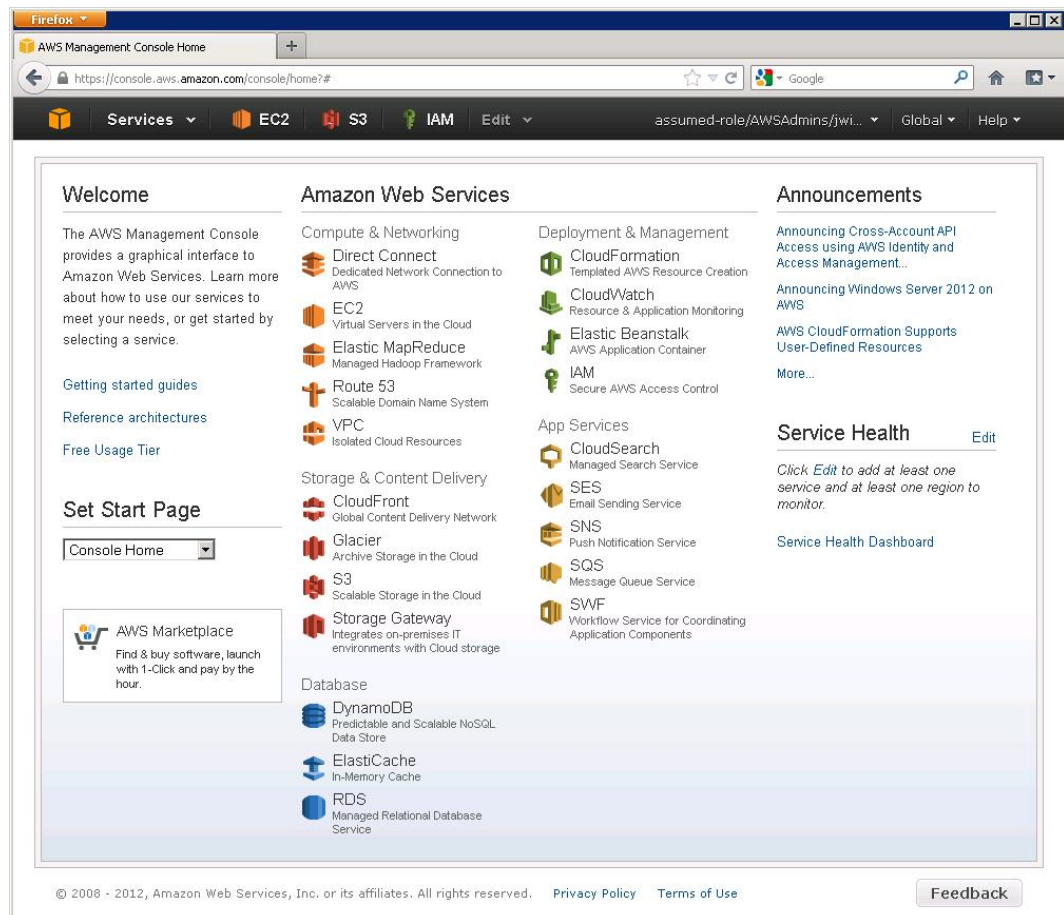
A. Regalado ve svém článku „Who coined Cloud Computing“ [5] uvedl, že „mnozí lidé se domnívají, že první nasazení moderního kontextu cloud computingu nastalo 9. srpna 2006, když Eric Schmidt (Google CEO) představil tento výraz na průmyslové konferenci.“ Je zajímavé, že vzniká nový model“, řekl Schmidt, „Nemyslím si, že lidé pochopí jak velká je to příležitost. Začíná s předpokladem, že datové služby a architektura by měla být na serverech. Nazýváme to cloud computing – měl by být někde v oblacích (cloud).“

Jeden z prvních milníků v historii cloud computingu byl příchod Salesforce.com v roce 1999, která zavedla koncept dodávky obchodních aplikací dostupných přes webovou stránku. Tato společnost vydláždila cestu specializovaným i mainstreamovým společnostem se softwarem, které mohly dodávat aplikace přes Internet, a hrála velmi důležitou úlohu při představování konceptu SaaS (Software as a Service) – software jako služba. SaaS model umožňuje společnostem přistupovat k software on-line a platit jen za služby a aplikace, které používají.

Další krok přinesla společnost Amazon v roce 2002 s Amazon Web Service, která poskytovala soubor cloudově založených služeb včetně úložného prostoru a výpočetního výkonu. Aplikace třetích stran mohly prohledávat a zobrazovat produkty z webové stránky Amazon a přidávat položky do nákupního košíku. První

verze AWS z roku 2002 byla zaměřená na tvorbu informací dostupných z Amazonu směrem k partnerům pomocí modelu webových služeb s programovou, vývojovou podporou a byla zaměřená na Amazon jako maloobchodní prodej.

V srpnu 2006 spustil Amazon komerční webovou službu, svůj Elastic Compute cloud (EC2). Toto řešení dalo uživatelům možnost ukládat data z venku, přejímat výpočetní cykly jako službu a poskytovat on-line služby pro další webové stránky nebo klientské aplikace. Pravděpodobně EC2 byl první široce přístupný cloud s infrastrukturou jako služba.



Obr. 1 – Okno správce služby Amazon Web Services

Spuštěním Google App Engine v dubnu 2008 se uskutečnil vstup první čistě technologické společnosti na trh cloud computingu. Služby Google Apps umožnily této společnosti začít nabízet obchodní aplikace dostupné přes webový prohlížeč.

Microsoft několik let neakceptoval web jako významný trh a pokračoval v desktopových aplikacích. Avšak v listopadu 2009 změnil Microsoft toto kritérium a spustil platformu cloud computingu s názvem Windows Azure. Tato platforma poskytuje jak PaaS tak též IaaS služby a podporuje různé programovací jazyky, nástroje a frameworky. V roce 2014 byla služba přejmenována na Microsoft Azure.

V prosinci 2013 byla spuštěna služba Google Compute Engine. Tato infrastruktura umožňuje uživatelům vytvářet a spouštět virtuální stroje na vyžádání s různými konfiguracemi.

V letech 2009-2010 si získal pozornost open source cloud. Existuje množství služeb cloud computingu, které jsou kompletně napsány v open source kódu nebo při nejmenším open source obsahují. Použití open source kódu v cloud computingu umožňuje vývojářům tvořit aplikace na existující aplikační infrastruktuře, využívaje nízké náklady, větší flexibilitu a pravděpodobně robustnější aplikace (s menším množstvím chyb) jako ty, které se stavějí na zelené louce. V mnoha modelech služeb cloud computingu existuje velké a rozmanité množství aplikací ať již v komerční nebo open source sféře jako například Apache Cloudstack, Eucalyptus, OpenNebula a OpenStack [6].



Příchodem úžasných aplikací od společností Microsoft, Google, Amazon, Apple, Cisco a dalších velkých IT společností mají za následek široké přijetí on-line služeb a představují relevantní přínos pro nasazování cloud computingu.

3 Vlastnosti cloud computingu

Cloud computing je model pro všudy přítomný, pohodlný, síťový přístup na vyžádání ke vzdálenému souboru konfigurovatelných výpočetních zdrojů (sítě, servery, disky, aplikace a služby), které mohou být okamžitě vyhrazeny a poskytnuty s minimálními nároky na správu nebo potřebu zásahu samotného poskytovatele. Podle NIST tento cloudový model sestává z pěti základních vlastností: samoobslužný systém na vyžádání, široký síťový přístup, sdružování zdrojů, rychlá elasticita, měření služby. Dále obsahuje několik společných vlastností jako škálovatelnost, virtualizace, orientace na služby, pružný výpočetní výkon, zvýšená bezpečnost, geografická distribuovatelnost, atd.

- Samoobslužné služby na vyžádání. Cloud computing poskytuje zdroje jako např. serverový čas a síťové úložiště na vyžádání, tzn. podle požadavků zákazníka. Příklady zdrojů zahrnují úložiště, procesor, paměti a rychlosti připojení. Zákazník si může jednostranně zajišťovat výpočetní prostředky. Toto je možné pomocí samoobsluhy a automatizace. Samoobsluhou se rozumí to, že zákazník sám vykonává všechny potřebné kroky k tomu, aby realizoval požadované služby. Jeho požadavky jsou automaticky zpracovány cloudovou infrastrukturou, bez lidské interakce na straně poskytovatele. Tyto vlastnosti zahrnují vysokou úroveň plánování, tedy zákazník si může kdykoli změnit své požadavky a očekává jejich realizaci do pár minut. Poskytovatel cloudového řešení by měl sledovat trendy ve využívání zdrojů a na jejich základě plánovat budoucí možné situace.
- Široký síťový přístup. Přístup k technologii je umožněn přes síť pomocí různých klientských platforem, díky použití standardních mechanismů. To nezahrnuje jen klasická zařízení (laptopy, pracovní stanice, atd.) ale též mobilní telefony, tenké klienty a mnohé další. Síť, úložiště a výpočetní zdroje byly ještě před několika lety omezeny a velmi nákladné. Postupem času se náklady spojené s těmito prostředky snižovaly v důsledku škálovatelnosti výroby a modifikací souvisejících technologií. Tak jak se zvyšovala přenosová rychlost, vzrůstal síťový přístup a škálovatelnost. „Široký síťový přístup“ je vnímán jako charakteristický rys a jako možnost.
- Sdružování zdrojů. Zdroje poskytovatele cloudové služby jsou děleny mezi několik uživatelů díky víceklientskému modelu vícenásobného nájemníka, tzv. „multi-tenant model“, s různými fyzickými a virtuálními zdroji dynamicky přidělovanými na vyžádání zákazníka. Tento koncept je základním předpokladem škálovatelnosti v cloudu. Prostředí vícenásobných nájemníků, kde někteří uživatelé sdílejí téměř shodné zdroje v cloudu s jinými uživateli, jsou základem veřejné cloudové infrastruktury. Při vícenásobném pronájmu je nemyslitelnou součástí zvyšování operačních nákladů, které mohou být kompenzovány jistou hardwarovou konfigurací a softwarovými řešeními jako např. aplikace a serverové profily. Dělení zdrojů poskytuje pocit nezávislosti na umístění. Uživatel neví, kde konkrétně se jeho zdroje nacházejí. Bez principu vícenásobného pronájmu a dělení zdrojů by cloud finančně nedával smysl.
- Rychlá elasticita. Elasticita je v zásadě přejmenování škálovatelnosti, která je schopna podle potřeby přidávat a nebo odebírat kapacitu, zejména výpočetní

výkon a paměť. Prostředky jsou vyčleněny a v některých případech automaticky poskytnuty tak, aby rychle reagovaly na požadavky zvyšování a snižování potřebných zdrojů. Pro uživatele se dostupné prostředky často jeví jako neomezené a mohou si jich zamluvit libovolné množství a času. Mnoho implementací je založeno na přidávání a odebírání uzlů, serverů nebo instancí do/z výpočetního fondu (cluster, farma). Dobře známým příkladem je přidávání kompenzace zátěže před farmu webových serverů, která distribuuje požadavky.

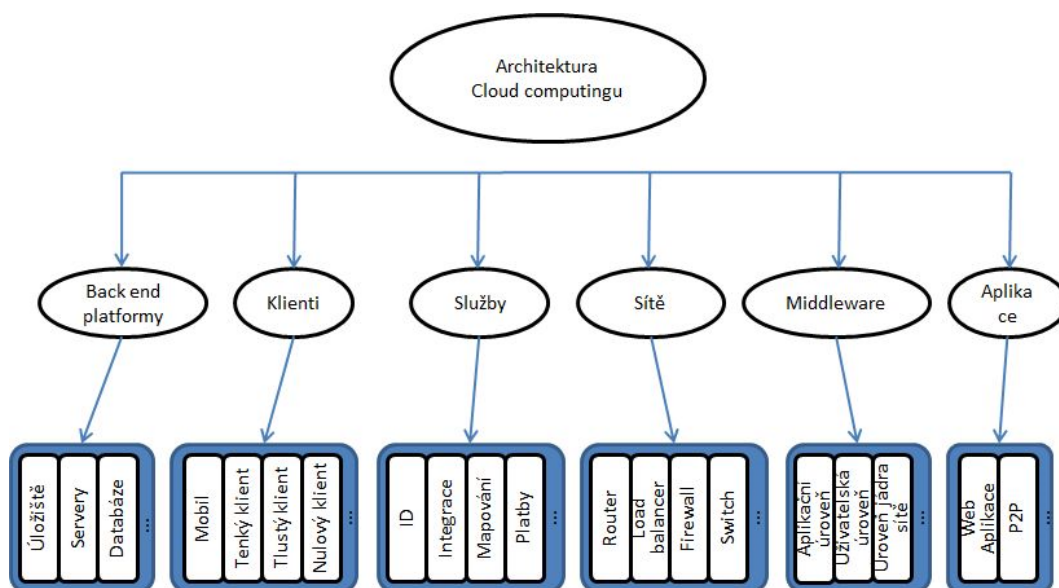
- Měření služby. Používané zdroje jsou monitorovány, řízeny a reportovány zákazníkovi, poskytujíc transparentní pohled pro uživatele i poskytovatele o spotřebě a nákladech. Toto je rozhodující pro fakturaci, kontrolu přístupu, optimalizaci zdrojů, plánování kapacit a další úlohy.

4 Komponenty a architektura cloud computingu

Při popisu architektury cloud computingu zdůrazňuje mnoho autorů použití a přístup výpočetních zdrojů založených na více serverech.



Nicméně, architektura cloudového řešení je struktura systému, který typicky obsahuje cloudové zdroje (back-end platformy, servery, úložiště), služby, síť, middleware a softwarové komponenty, jejich viditelné vlastnosti zvenku a vztahy mezi nimi [7].



Obr. 2 – Komponenty cloud computingu

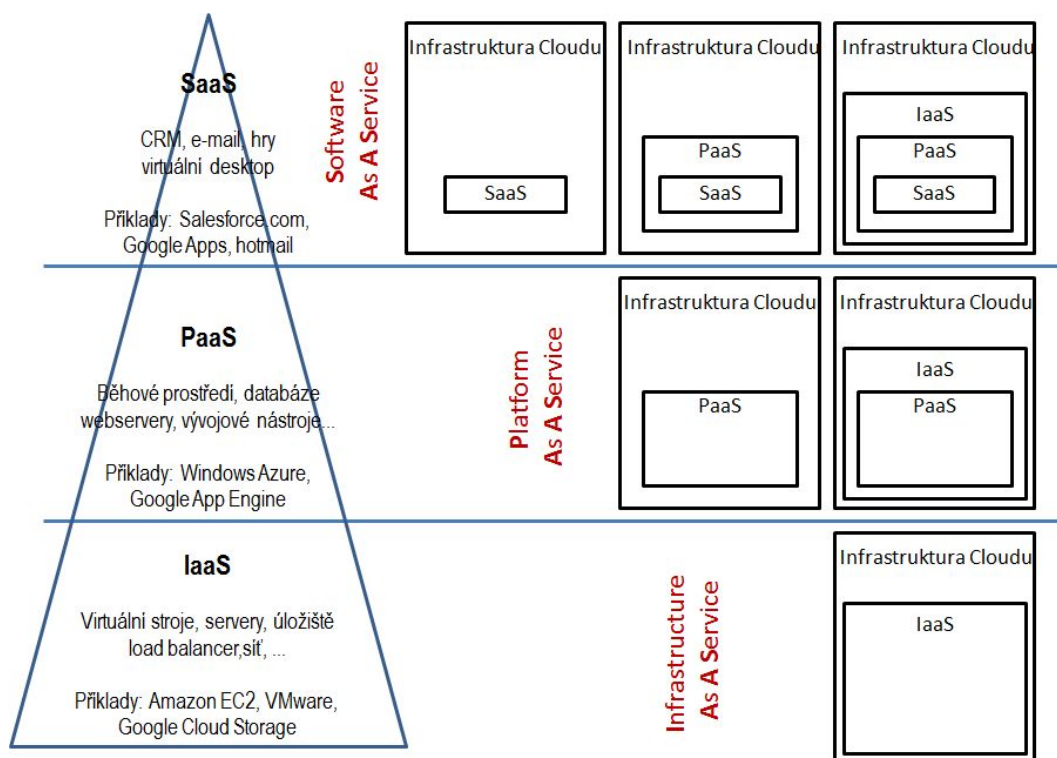
- Back-end platforma. Tyto servery jsou velmi rozlehlé a dovedou držet velké množství dat a mohou být umístěné kdekoli na světě. Často jsou servery v geograficky vzdálených lokalitách, ale chovají se, jako by byly vedle sebe. Obvykle existuje i centrální server, který spravuje celý systém, monitoruje provoz a požadavky klientů, aby se ujistil, že vše běží v pořádku.
- Cloudoví uživatelé mohou přistupovat ke cloudovým zdrojům pomocí klientů (tlustých, tenkých, nulových klientů, tabletů, mobilních zařízení, ...). Tyto klientské platformy spolupracují s cloudovým datovým úložištěm prostřednictvím aplikace (middleware), webového prohlížeče nebo virtuální spojení.
- Síť: Z klientské strany je využívání služeb cloud computingu pro podniky hrozbou, že se změní IT servery za síť a správa serverů za správu sítě. Z toho důvodu plyne několik požadavků na síť. Na druhé straně poskytovatel služby musí zajistit, aby veškerá komunikace probíhala hladce, jednoduše a s ohledem na bezpečnost. Je důležité mít inteligentní, spolehlivou a funkční síť, která poskytuje prostor pro inovace.

- Middleware je software, který vytváří spojení mezi libovolnými dvěma klienty, servery, databázemi nebo dokonce aplikacemi. Cloudový middleware poskytuje uživatelům několik funkcionalit, které jim pomáhají při tvorbě obchodních aplikací; napomáhání souběžnosti, transakce, řazení a správa.
- Služby. Cloudové služby jsou služby, které podporují řešení založené na cloudu, jako např. správa identit, integrace služba-služba, mapování, fakturace, platby, vyhledávání ...
- Aplikace. Cloudová aplikace (Cloud App) je aplikační program, který běží v cloudu s některými vlastnostmi desktopové aplikace a vlastnostmi webové aplikace. Obvykle jsou tyto aplikace vytvořeny v integrovaném prostředí; příkladem je Google App Engine, který umožňuje uživatelům vytvořit aplikace na těch samých škálovatelných systémech jako Google aplikace.

5 Servisní modely cloud computingu

Cloud computing nabízí organizacím nové možnosti v souvislosti s tím, jak provozovat infrastrukturu, šetřit náklady a delegovat závazky na třetí stranu – poskytovatele. Stal se ucelenou částí technologie a obchodního modelu a nutí obchod k tomu, aby se adaptoval na nové technologické strategie. Taktéž poptávka po cloud computingu zrychlila vývoj nových tržních nabídek a reprezentuje rozličné cloudové služby a modely doručení služby k zákazníkovi. Tyto modely významně rozšiřují rozsah dostupných možností a organizaci zadání s otázkou, který model cloud computingu využívat.

Modely služeb popisují, jak jsou cloudové služby dostupné klientům. Podle NIST existují tři modely služeb: SaaS (software jako služba), PaaS (platforma jako služba) a IaaS (infrastruktura jako služba), které jsou popsány v následujících kapitolách. Ve skutečnosti je nejzákladnější model služeb kombinací IaaS, PaaS a SaaS. Tyto modely služeb mohou mít vzájemnou synergii a být nezávislé; jako příklad PaaS je závislá na IaaS, protože aplikační platformy potřebují fyzickou infrastrukturu.



Obr. 3 – Servisní modely. Převzato z [8]

Dnes si společnosti víc uvědomují hodnotu a šetření zdrojů softwaru a platformových služeb než infrastruktury. Z toho důvodu je IaaS model schopný držet ztrácející podíl na trhu oproti PaaS a SaaS. V blízké budoucnosti se očekává významný počet tržních konsolidací s několika významnými hráči, kteří si ponechají kontrolu až do konce [9].

5.1 Software as a Service

SaaS (*software jako služba*): je softwarový distribuční model, ve kterém jsou aplikace hostované samotným prodejcem nebo poskytovatelem služeb a jsou zpřístupněny zákazníkům přes síť, typicky přes internet. Tato vlastnost eliminuje potřebu instalovat software na straně klienta a může být užitečná pro mobilní nebo dočasné pracovníky.

E-mail je jednoduchý příklad SaaS. Má-li uživatel poskytovatele služeb, vyžaduje desktopovou nebo mobilní aplikaci na přístup k e-mailu. Jinak jej může hostovat na individuálním serveru. Je důležité poukázat na to, že uživatel nemůže spravovat ani řídit infrastrukturu cloudu, nebo specifické vlastnosti aplikace s výjimkou limitovaného nastavení konfigurace aplikace.



Výhody SaaS jsou:

- Šetření nákladů: Malé nebo žádné kapitálové investice
- Flexibilita: nabízená jako služba na vyžádání
- Stabilita: SaaS aplikace jsou instalované na profesionálním, zabezpečeném a redundantním hardware.
- Okamžité nasazení: Od žádného po velmi malý čas na vyhrazení a nasazení
- Dostupnost: jediná potřebná věc je internetové připojení
- Nové aktualizace: Poskytovatelé služeb aktualizují řešení a to je automaticky dostupné pro zákazníky; náklady s tím spojené, jsou mnohem nižší než u tradičních modelů.



Kromě nedostatečné kontroly, je jednou z hlavních nevýhod fakt, že SaaS aplikace nemusí mít stejné vlastnosti jako non-SaaS aplikace. Funkcionalita není často přepracovaná nebo úplná. Nicméně tento problém bude časem zeslaben. Vývojové nástroje per SaaS aplikace se stávají mnohem více způsobilé. Konečně rychlost může být nevýhodou; všeobecně jsou SaaS aplikace pomalejší než jejich non-SaaS ekvivalenty.

Příklady poskytovatelů služeb SaaS:

- Google Apps: poskytuje webové kancelářské nástroje jako e-mail, kalendář a dokumenty
- Salesforce.com: poskytuje plné **CRM** (*customer relationship management*) aplikace
- Zoho.com: poskytuje velký soubor webově-orientovaných aplikací, většinou pro firemní účely

5.2 Platform as a Service

PaaS (*Platforma jako služba*): je kategorie cloud computingu, která poskytuje platformu a prostředí tak, aby umožnila vývojářům vytvářet aplikace a služby přes Internet. PaaS služby jsou hostované v cloudu a dostupné přes webový prohlížeč. Obvykle se jedná o způsob pronájmu hardware, operačního systému, úložiště a síťové kapacity přes internet.

Model služeb poskytuje zákazníkům pronajmout si virtualizované servery a příslušné služby pro běh vlastních aplikací, které jsou vytvořeny pomocí programovacích jazyků, knihoven, služeb a nástrojů podporovaných samotným poskytovatelem. Platformy pro vývoj aplikací povolují uživatelům vytvářet a hostovat aplikace větších rozměrů, než by byli sami schopni zvládnout. Poskytovatelé PaaS mohou asistovat vývojářům od konceptu jejich originální myšlenky až po vytvoření aplikace, její testování a nasazení. To všechno je dosaženo řízeným mechanismem.

Zákazník nespravuje ani neřídí infrastrukturu cloudu včetně sítě, serverů, operačních systémů nebo úložiště, ale má kontrolu přes nasazenou aplikaci a konfigurační nastavení v hostovaném prostředí. Profitují z nízkých ekonomických nákladů, které vycházejí ze sdílení infrastruktury mezi více uživateli. Klient služby PaaS platí obecně za prostředky, které ve skutečnosti čerpá.

Příklady prostředků, které mohou být obsaženy v PaaS:

- Operační systém
- Skriptovací prostředí na serveru
- Systém na správu databází
- Serverový software
- Podpora
- Úložiště dat
- Síťový přístup
- Nástroje na návrh a vývoj
- Hosting



Výhody PaaS jsou:

- Vývojáři software mohou používat personální PaaS prostředí na každé úrovni procesu vývoje, testovat a nakonec hostovat svoji aplikaci.
- Tým může spolupracovat na dálku. Kdokoli kdekoli je schopen pracovat na projektu.

- Flexibilita; zákazníci mají kontrolu přes různé nástroje, které jsou nainstalované v rámci své platformy a mohou vytvořit platformu, která se hodí jejich specifickým požadavkům
 - Šetření nákladů: netřeba investovat do fyzické infrastruktury.
 - Maximalizace provozu: poskytovatelé PaaS by měli mít nástroje, technologie a zkušenosti k pomoci uživatelům předejít neplánovaným výpadkům.
 - Jednoduché škálování. Vlastnosti PaaS mohou být změněny, jestliže je potřeba.
-



Jedna z nevýhod PaaS je, že v závislosti na nabídce společnosti, poskytuje možnost uzavřít uživatele do specifického softwarového prostředí, jazyka nebo rozhraní. To mohou zabezpečit někteří poskytovatelé, ne však všichni.

Příklady PaaS:

- Google App Engine: poskytuje uživatelům kompletní vývojářský zásobník a umožňuje jim, aby jejich aplikace běžely na infrastruktuře Google
- Akamai EdgePlatform: poskytuje velikou distribuovanou počítačovou platformu, ve které mohou organizace nasazovat své vlastní webové aplikace; zaměření na analýzu a monitoring
- Microsoft Azure: poskytuje výpočetní výkon a služby datového úložiště založené na vývojové platformě Windows
- Yahoo! Open Strategy (Y!OS): poskytuje uživatelům prostředky na vývoj webových aplikací založených na existující službě Yahoo!

5.3 Infrastructure as a Service

IaaS (*infrastruktura jako služba*): je model nasazení, ve kterém pronajaté zdroje tvoří operační systémy, zabezpečení, síť, úložiště a servery pro vývoj aplikací, služeb a pro nasazování vývojových nástrojů, databází, atd. Poskytovatel služeb vlastní zařízení a je zodpovědný za hostování, běh a správu. Klient typicky platí podle využití nabízených zdrojů. Místo připravených aplikací a služeb je poskytována síť; nejpoužívanější IaaS systémy obsahují virtuální servery, kompenzaci přetížení a síťové připojení.

IaaS umožňuje organizacím a vývojářům rozšiřovat svoji IT infrastrukturu na požádání. Poskytovatel cloudového řešení má soubor virtualizovaných výpočetních zdrojů a disků, které může uživatel využívat. Toto je computing na vyžádání a má na starosti různorodost ve výpočetních výkyvech. Fyzicky je soubor hardwarových zdrojů složen z velkého množství serverů a sítí, obvykle distribuovaných mezi několika datovými centry. Poskytovatel je zodpovědný za celkovou jejich správu. Klientovi, na druhé straně, je dán přístup k virtualizovaným komponentám pro sestavení vlastní IT platformy. Klient nespravuje ani neřídí infrastrukturu cloudu ale má kontrolu operačního systému, disku a nasazených aplikací; a možnost omezené kontroly vybraných síťových komponentů (servery, firewally...).



Výhody IaaS jsou:

- Rychlý a jednoduchý přístup k podnikovým řešením
- Škálovatelnost; zdroje jsou stále dostupné, a pokud klient vyžaduje víc zdrojů, má je okamžitě k dispozici, pokud zdroje již nepotřebuje, může požadavky snížit
- Jednoduchost: poskytovatel má na starosti správu zdrojů, obstarávání hardware a software, záplaty a všechny komplexní úkony spojené s infrastrukturou
- Žádné investice do hardware; fyzický hardware, který podporuje IaaS služby je instalován a spravován poskytovatelem cloudových služeb, šetří čas a náklady klienta
- Nezávislost na umístění; služba může být přístupná z libovolného místa, pokud má přístup na internet a bezpečnostní protokol cloudu to povolí
- Fyzická bezpečnost umístění datového centra; služby dostupné přes veřejný cloud nebo privátní cloudy hostované externě u poskytovatele cloudu, výhody fyzické bezpečnosti pro servery v rámci datového centra
- Rychlé nasazení: malý nebo žádný čas pro nasazení.

Pro větší obchody je hlavní výhodou poslední uvedený bod; je spřažen s včasným nasazením při nepředvídaných okolnostech a potřebách.



Hlavní nevýhodou IaaS je podnikatelské riziko. I s velkým úsilím, auditem a proaktivní správou, vyžaduje IaaS důvěru v infrastrukturu prodejce, dostupnost, datová bezpečnost, atd.

Příklady poskytovatelů IaaS:

- Amazon Elastic Compute Cloud (EC2): poskytuje uživatelům speciální virtuální stroj (AMI), který může být nasazen a běžet na infrastruktuře EC2
- Amazon Simple Storage Solution (S3): poskytuje uživatelům přístup do dynamicky škálovatelného úložiště
- Microsoft Live Mesh: poskytuje uživatelům přístup do distribuovaného souborového systému; zaměřeného na individuální použití
- IBM Computing on Demand (CoD): přístup ke konfigurovatelným serverům plus přidaná hodnota služeb jako datové úložiště

Společně s dalšími dvěma formami cloud hostingu, může být IaaS využívána firemními zákazníky na tvorbu cenově výhodných a jednoduše škálovatelných IT řešení, kde komplexnost a výdaje spojené se správou hardware jsou přenechány poskytovateli řešení. Jestliže škála obchodních zákaznických operací fluktuuje nebo má výhled expandovat, mohou uživatelé čerpat cloudové zdroje podle potřeby raději než aby je nakupovali, instalovali a integrovali hardware svépomocně.

6 Modely nasazení

Používají se obvykle čtyři modely nasazení cloudu: privátní, veřejný, hybridní a komunitní. Poslední z nich se používá nejméně.

- Privátní cloud je vystavěn a spravován v rámci jediné organizace. Organizace používají software, který umožňuje funkcionalitu cloudu, například VMware.
- Veřejný cloud sestává z výpočetních zdrojů poskytnutých třetí stranou. Mezi nejpoblárnější veřejné cloudy patří Amazon Web Services, Google AppEngine a Microsoft Azure.
- Hybridní cloud je kombinací výpočetních zdrojů poskytnutých privátními i veřejnými cloudy.
- Komunitní cloud sdílí výpočetní zdroje mezi vícero organizacemi a může být spravován nejen IT zdroji z organizací, nýbrž též jinými poskytovateli.

Dosud dominantní veřejný model nasazení cloudu se bude dále rozšiřovat. Privátní a hybridní modely nasazení zůstanou sice v následujících letech používané, ale jejich podíl na trhu bude neustále klesat. Z dlouhodobého hlediska budou privátní a hybridní modely cloudu využívány zřejmě jen na specifické obchodní řešení.

6.1 Veřejný cloud

Veřejné cloudy poskytují široké veřejnosti poskytovatelé služeb, kteří spravují cloudovou infrastrukturu. Veřejní poskytovatelé cloudů jako Amazon AWS, Microsoft a Google vlastní a řídí infrastrukturu a přes internet nabízí otevřený přístup široké veřejnosti. V takovémto modelu nemohou zákazníci vědět ani neovlivnit, kde se infrastruktura nachází. Je potřeba poznamenat, že všichni zákazníci veřejného cloudu sdílejí tu samou infrastrukturu s omezenou konfigurací, bezpečnostní ochranou a variantami dostupnosti. Jako příklady mohou být uvedeny služby určené pro širokou veřejnost, služby on-line ukládání fotek, e-mailové služby či stránky sociálních sítí. Ve veřejném cloudu však mohou být poskytovány i služby pro podniky.

Ve veřejných cloudech se zdroje nabízí jako služba. Uživatelé mohou měnit své potřeby na požádání a nemusí kvůli tomu nakupovat hardware. Poskytovatelé veřejného cloudu spravují infrastrukturu a rozdělují ji podle kapacitních požadavků uživatelů.



Zákazníci veřejných cloudů využívají ekonomičtější možnosti růstu, protože náklady na infrastrukturu jsou rozdělené rovnoměrně mezi všechny uživatele, díky čemuž může každý klient fungovat samostatně, nízkonákladově, systémem „pay-as-you-go“. Další výhodou veřejných cloudových infrastruktur je, že jsou mnohem větší než vnitřní podnikové cloudy. Proto mají klienti k dispozici možnost plynulého škálování na požádání. Tyto cloudy poskytují nejvyšší úroveň efektivnosti sdílených prostředků.

Veřejný cloud je jasnou volbou, když:

- je standardizovaná zátěž pro aplikace využívaná množstvím osob, např. e-mail.
- je třeba testovat a vyvíjet aplikační kód.
- je nutné postupně navyšovat kapacitu (schopnost přidat výpočetní zdroje během špiček),
- se pracuje na společných projektech.

6.2 Privátní cloud

V privátním cloudu využívá celou infrastrukturu výhradně jediný klient nebo organizace. Není sdílená s jinými organizacemi, avšak může obsluhovat více zákazníků (např. obchodní jednotky). Infrastruktura může být umístěná interně nebo externě a může ji spravovat buď organizace sama, třetí strana anebo jejich kombinace. Umožňuje organizacím ukládat data a aplikace v cloudu, který je bezpečnějším a lépe řízeným prostředím v porovnání s veřejným cloudem. Zdroje jsou nasazené za firewallem a přístup k nim může být zabezpečen pomocí soukromých linek nebo zabezpečených šifrovaných spojení přes veřejné sítě tak, aby přístup k nim měli pouze konkrétní klienti, kteří s nimi mohou pracovat. Cílem těchto mechanismů je minimalizovat bezpečnostní rizika a omezit přístup jen pro vybrané klienty.

Podle umístění existují dvě varianty privátních cloudů [10]:

Cloud ve vlastních prostorách: Tento druh cloudu je umístěný přímo v prostorách organizace. Tato možnost je vhodná pro organizace, které investovaly do značného serverového a ukládacího hardware, chtějí využít tuto investici a použít hardware na privátní cloud, například pro aplikace vyžadující kompletní kontrolu a konfigurovatelnost infrastruktury a bezpečnosti.

Externě umístěný privátní cloud: externě umístěné cloudy se nacházejí u třetí strany, která se specializuje na cloudovou infrastrukturu. Poskytovatel služeb zřídí vyhrazené cloudové prostředí s úplnou zárukou soukromí. Tento formát se doporučuje organizacím, které preferují nevyužívání veřejné cloudové infrastruktury z obav spojených se sdílením fyzických zdrojů.



Spuštění projektu privátního cloudu vyžaduje významnou snahu o virtualizaci prostředí. Privátní cloudy jsou dražší, avšak bezpečnější v porovnání s veřejnými. Významná část osob zodpovědných za rozhodnutí v IT se zaměřují výhradně na privátní cloud, neboť tyto cloudy poskytují nejvyšší úroveň bezpečnosti a řízení.

Privátní cloud je možné označit za nejlepší řešení, jestliže:

- je potřeba vysoké míry kontroly,
- je kriticky důležitá bezpečnost dat a soukromí,
- je vyžadovaná nezávislost dat společně s výhodami cloudu.

6.3 Komunitní cloud

Komunitní cloud je model cloudové služby s více vlastníky, kterou sdílí několik organizací ze specifické skupiny s podobnými nároky na službu (např. cíle, bezpečnostní požadavky a vzájemný soulad). Tyto organizace nebo spíše komunity mají podobné nároky na cloud a jejich hlavním cílem je spolupracovat na dosažení svých obchodních cílů. Komunitní cloud má svoje vlastní úskalí jako alokace nákladů, zodpovědnosti, řízení a bezpečnosti.

Náklady jsou rozloženy mezi menší počet uživatelů než u veřejného cloudu (ale větší než u privátního cloudu). Potenciál úspor nákladů tedy není tak vysoký. Cloud mohou spravovat přímo organizace nebo třetí strana, a umístěn může být v prostorách organizace nebo mimo ní.

Obecně jsou veřejné cloudové služby finančně výhodnější a škálovatelnější než privátní cloudy, avšak jsou méně bezpečné.



Cílem komunitních cloudů pro dotčené organizace je sloučení výhod veřejného cloudu s vyšší úrovní soukromí, bezpečnosti a souladu s vnitřními pravidly, které jsou obvykle doménou privátního cloudu.

Výhody bezpečnosti v prostředí komunitního cloudu využívají například vládní, zdravotnické nebo telekomunikační komunity organizací, ale též regulované soukromé podniky. Místo pouhého využívání prostoru ve veřejném cloudu mohou organizace testovat a pracovat v cloudové platformě, která je bezpečná, vyhrazená pouze pro ně a dokonce splňuje specifické předpisy.

6.4 Hybridní cloud

Hybridní nebo kombinovaný cloud je kombinací různých metod řízení zdrojů, například kombinování veřejných a komunitních cloudů. Na hybridní cloudy je možno též nahlížet jako na kombinaci dvou nebo více cloudů (privátních, komunitních a nebo veřejných), které jsou vzájemně provázané a poskytují tak výhody více modelů nasazení, s použitím standardizované nebo proprietární technologie, která umožňuje přenositelnost dat a aplikací. Všechny tyto techniky se mohou použít i u externích poskytovatelů cloudových řešení buď zcela, nebo částečně, což zvyšuje flexibilitu computingu. Hlavní myšlenkou hybridního cloudu je kombinovat několik cloudových modelů na vytvoření řešení na míru požadavkům příslušné organizace.

Architektura hybridního cloudu vyžaduje mít cloudovou infrastrukturu přímo v prostorách organizace a zároveň servery umístěné jinde. Je možno ji implementovat různými způsoby. Organizace může mít například data a aplikace umístěné v cloudu, který zachovává kontrolu nad topologií sítě organizace a jej vnitřní politikou. Zároveň si může zachovat existující fyzickou infrastrukturu (ačkoli ta se nedá dynamicky měnit) a půjčovat si další zdroje podle potřeby.



Hybridní cloudy umožňují společnosti zachovávat všechny části jejího podnikání v tom nejefektivnějším prostředí. Krom toho jsou tyto modely lehké rozšiřitelné, cenově efektivní (méně citlivá data je možno přemístit z privátního cloudu do veřejného cloudu), bezpečné a flexibilní.



Nevýhodou je, že organizace musí sledovat více cloudových bezpečnostních řešení a zajistit, aby všechny složky podniku mohly vzájemně komunikovat.

Hybridní cloud je vhodnou možností v případě, že:

- Společnost chce používat veřejný cloud na testování a vývoj a hostovaný privátní cloud ve společnosti chce využívat na produkční nasazení.
- Společnost používá veřejné cloudy pro aplikace směřující externě, zatímco hostovaný privátní cloud využívá na interní aplikace.
- Společnost chce používat veřejný cloud na kontakt se zákazníky, ale jejich citlivá data chce udržovat v zabezpečeném privátním cloudu.

7 Použití a aplikace

Cloud computing může podporovat prakticky jakoukoli aplikaci. Některé úlohy jsou však vhodnější pro nasazení do cloudu z organizačního nebo technického hlediska. Dva nejlepší příklady pro využití cloud computingu jsou:

Správa velkého množství dat. Cloud computing je jako stvořen na analytické zpracování velkého množství dat. Vzhledem k pružné výpočetní kapacitě a poskytování výkonu na požádání, je analýza dostupná více týmům v organizaci. Kromě toho je cloud užitečné řešení, je-li potřeba větší množství výpočtů na řešení složitých úloh, nebo je potřeba spolupráce více vývojářů. Cloud computing umožňuje efektivnější vykonávání výpočtů pomocí centralizace ukládání dat.

Testování a vývoj v cloudu. Vývojové týmy využijí pružnost tvorby virtuálních strojů za několik minut. Cloud computing nevyžaduje od organizací, aby si vývojové prostředí zřizovaly pomocí fyzických zařízení, značné pracovní síly a času. Okrem toho může organizace dostat aplikace do produkčního prostředí rychle a škálovat je podle potřeby.

Další relevantní možnosti použití jsou:

- Ukládání souborů a sdílení
- Zálohování a obnovování po haváriích
- CRM
- Hosting web stránek

Typické aplikace:

- Sociální sítě
- e-mailové stránky
- vyhledávače
- komunikační řešení (např. Skype)
- aplikace na sledování času
- Správa poznámek (např. Evernote)
- Tvorba a sdílení kancelářských dokumentů (např. Google Apps)

8 Výhody a nevýhody cloud computingu

Mnoho uživatelů a malých i velkých podniků dnes místo tradičních alternativ využívá cloud computing přímo (např. Google nebo Amazon) nebo nepřímo (např. Twitter).

Cloudy nabízí uživatelům množství různých výhod. Jednou z nejdůležitějších je snížení nákladů a složitosti z vlastnictví a používání počítačů a sítí. Uživatelé cloudu nemusí investovat do informační infrastruktury, kupovat hardware nebo platit licence za software. Dále existují poskytovatelé cloudu, kteří se specializují na konkrétní oblasti (jako např. e-mail), což může společností přinášet užitečné a pokročilé služby.

Mezi další výhody pro klienty patří škálovatelnost, spolehlivost a efektivita. Škálovatelnost znamená, že cloud computing není omezený výkonnostně ani kapacitně. Cloud je spolehlivý díky tomu, že poskytuje přístup k aplikacím a dokumentům kdekoli na světě prostřednictvím internetu. Cloud computing se často považuje za efektivní, protože dovoluje organizacím uvolnit zdroje a použít je na inovace a vývoj produktů. Navíc se informace z cloudu lehce neztratí.

Dále je uveden seznam některých nejdůležitějších výhod plynoucích z používání cloud computingu:

- Dostupnost a univerzální přístup. Cloud computing umožňuje vzdáleným zaměstnancům přístup k zdrojům a aplikacím v jakémkoli čase přes běžné internetové připojení.
- Výběr aplikací. Ten umožňuje pružnost uživatelům cloudu ve výběru a zkoušení toho, co nejvíc vyhovuje jejich potřebám. Cloud computing taktéž umožňuje podnikům používat, přistupovat a platit jen za to, co využívají, a to s rychlým časem implementace.
- Spolupráce. Uživatelé začínají cloud vnímat jako způsob souběžné práce se společnými daty a informacemi.
- Snížení nákladů. Model plat'-za-použití (pay-per-usage) na rozdíl od vlastního hostingu dovoluje organizaci platit jen za zdroje, které potřebuje, prakticky bez investic do fyzických zdrojů, které jsou dostupné v cloudu.
- Pružnost. Poskytovatel transparentně spravuje klientovo využití zdrojů na základě dynamicky se měnících potřeb.
- Flexibilita. Cloud computing umožňuje klientům rychle a jednoduše si měnit aplikace tak, aby používali takovou, která nejvíce vyhovuje jejich potřebám.
- Potenciál být ekologičtější a ekonomičtější. Přiměřené množství energie potřebné na výpočetní činnost vykonanou v cloudu je velmi menší než při vykonání ve vlastním prostředí. Je to tak díky tomu, že více organizací může společně sdílet fyzické zdroje.
- Snížení rizika. Organizace mohou používat cloud na testování nápadů a nových konceptů dříve, než by značně investovaly do technologie.

- Škálovatelnost. Uživatelé mají přístup k velkému množství zdrojů, které jsou škálovány podle jejich potřeb.
- Aktuální software. Poskytovatel cloudu je schopný aktualizovat software při zachování zpětné vazby na předešlé verze software.
- Virtualizace. Každý uživatel má svůj pohled na dostupné zdroje bez ohledu na to, jak uspořádané jsou fyzické zařízení. Proto má poskytovatel perspektivu obsloužit větší množství uživatelů s menším množstvím fyzických zdrojů.

Oproti tomu existuje několik problémů, které mohou bránit organizaci v používání cloud computingu. Následuje seznam takovýchto omezení:

- Interoperabilita. Dosud nebyly definovány univerzální standardy a/nebo rozhraní, což může vést k riziku uzamčení organizace u jediného poskytovatele (tzv. vendor lock-in).
- Zpoždění. Veškerý přístup ke cloudu se děje prostřednictvím internetu, což přináší zpoždění v každé komunikaci mezi uživatelem a poskytovatelem.
- Omezení platformy nebo jazyka. Někteří poskytovatelé cloudu podporují pouze vybrané platformy a jazyky.
- Regulace. V komunitě cloud computingu, zejména u organizací spravujících citlivá data, existují obavy o soudní pravomoci, ochranu dat, spravedlivé zacházení s informacemi a mezinárodní přenos dat.
- Spolehlivost. Mnoho existujících cloudových infrastruktur využívá lacinější hardware, který může nečekaně selhat.
- Kontrola zdrojů. Množství kontroly, které má uživatel nad poskytovatelem cloudu a jeho zdroji, se mezi jednotlivými poskytovateli značně liší.
- Bezpečnost. Hlavní obavou je soukromí dat; uživatelé nemají kontrolu ani povědomí o tom, kde jsou jejich data skutečně uložena. Nicméně, z pohledu forenzní bezpečnosti může využívání cloud computingu poskytnout vyhrazené, při platbě-za-použití, forenzní obrazy virtuálních strojů, které jsou dostupné bez odpojení infrastruktury. To vede ke kratšímu času odpojení potřebného pro forenzní analýzu. Auditní záznamy mohou být taktéž ukládány finančně efektivněji, a tedy je možná podrobnější analýza auditních záznamů bez ovlivnění výkonu [11].

9 Bezpečnost v cloudu. Možná rizika



I přes mnoho výhod, existují i obavy o soukromí a bezpečnost v cloudu. Data se přenáší přes internet a ukládají na vzdálených místech. Poskytovatelé cloudu obsluhují množství zákazníků najednou. Toto všechno může zvýšit míru vystavení se možným průnikům do soukromí, ať již náhodně nebo cíleně. Je nutno zabezpečit, aby s osobními informacemi bylo nakládáno zodpovědně [12]. Obavy o bezpečnost mohou zvýšit dynamický charakter cloudového prostředí. Jednou z hlavních výhod cloudu je rychlost, s jakou mohou poskytovatelé cloudu upravovat, vyvíjet a měnit svoji nabídku. Vždy existuje kompromis mezi stupněm bezpečnosti a požadavky na rychlost a flexibilitu.

Cloud computing s sebou nese několik rizik spojených s ochranou dat pro zákazníky i pro poskytovatele cloudu. V některých případech může být pro zákazníka cloudu (jako správce dat) složité efektivně kontrolovat, jakým způsobem poskytovatel cloudu zachází s daty, aby se ubezpečil, že se s daty nakládá zákonným způsobem. Tento problém je zjevnější v případě vícenásobných přenosů dat, např. mezi propojenými cloudu.

Soukromí, včetně potřeby chránit informaci o identitě, je základní otázkou úspěchu nasazení cloudu. Mnoha organizacím se nelíbí uchovávat svá data a aplikace na systémech, které jsou umístěny mimo jejich datová centra. Riziko vystavení nebo nepovoleného přístupu k citlivým datům roste v případě, že pracovní činnosti migrují směrem ke vzdálené infrastruktuře.

Vzniklo též mnoho obav, že cloud computing může vést k tzv. „function creep“ – použití dat poskytovateli cloudu, které nebylo očekávané během získávání původních dat, a na které nebylo získané povolení. Požádá-li někdo o odstranění cloudového zdroje, nemusí to, podobně jako u většiny operačních systémů, vést ke skutečnému vymazání dat. Taktéž adekvátní nebo včasné odstranění dat může být nemožné (či nežádoucí z pohledu zákazníka), protože existují další kopie, které jsou nedostupné, nebo proto, že disk, který se má zničit, obsahuje data jiných klientů. Vyšší riziko pro zákazníka představují vícenásobné pronájmy a znovu použití hardwarových zdrojů než vyhrazený hardware. Vzhledem k tomu, jak laciné je ukládání dat, je malý zájem na odstranění informací z cloudu, a více důvodů na jeho další využití.

Poskytovatelé cloudových služeb musí své zákazníky ujistit a poskytnout jim vysoký stupeň transparentnosti operací a zabezpečit soukromí dat. Nástroje na ochranu soukromí musí být přímo vestavěné ve všech bezpečnostních řešeních.

10 Závěr

Cloud computing je nově vznikající a rapidně se vyvíjející model s novými možnostmi a způsoby použití. Cloud computing představuje cloudovou alternativu k něčemu, co by organizace obvykle spravovala vlastními prostředky s použitím dynamicky škálovatelných a často virtualizovaných zdrojů poskytovaných jako služba přes internet či intranet. Například webmail je cloudová alternativa k hostingu na vlastním e-mailovém serveru.

Většina služeb cloud computingu je přístupná pomocí web prohlížeče přes jakékoli připojené zařízení (mobil, tablet, osobní počítač...). Proto cloudové služby nevyžadují, aby měli uživatelé sofistikovaný počítač schopný spouštět speciální software. Díky rozhraní orientovanému na uživatele je cloudová infrastruktura a podpora aplikací pro uživatele transparentní.

Cloud computing má potenciál stát se přelomovou silou ovlivňující nasazení a využití technologií; cloud prakticky mění způsob, jakým mnoho organizací spravuje informační technologie. Podle perspektivy a situace v organizace či u jednotlivce, to představuje příležitost a zároveň i krizi. Této změně je možno odolávat, i když je to dobrá myšlenka a funguje to. Společnosti mají mnoho cest jak přistupovat k cloudu, včetně jeho infrastruktury, platforem a aplikací, které jsou dostupné poskytovateli cloudu jako on-line služby.

Jedněmi z hlavních obav jsou bezpečnost a soukromí. Tyto obavy závisí na typu společnosti. V případě velkých organizací se značnými zdroji, které mohou vyhradit na sofistikovaný program informační bezpečnosti, je potřebné překonat množství výzev v oblasti bezpečnosti, soukromí a spolupráce. Proti tomu, a v případě malých a středních podniků (SME – SMB – MSP), může bezpečnost cloud computingu vypadat atraktivně v porovnání se zdroji, které si společnosti mohou v dnešní době dovolit utratit za informační bezpečnost.