

Mraky zastřeno

Soukromí v cloud computingu: možnosti a implikace

Joss Wright (joss.wright@oii.ox.ac.uk)

1 Úvod

„Cloud computing je model umožňující pohodlný, on-demand (na vyžádání) síťový přístup ke sdíleným výpočetním zdrojům (např. sítím, serverům, paměťovým úložištím, aplikacím a službám), které lze rychle objednávat a rušit s minimálním úsilím managementu či interakcí poskytovatele služeb.“

Definice cloud computingu podle instituce NIST, viz [8]

Informační technologie a komunikační infrastruktura, která byla vytvořena kolem nich, jsou velmi důležité z hlediska mnoha aspektů globální společnosti. Vlády, podniky a jednotlivci spoléhají na počítačové sítě pro komunikaci, ukládání a zpracování informací.

Cloud computing je založen na poskytování služeb informačních technologií prostřednictvím specializované třetí strany, spíše než jejich tvorbou a správou interně samotnou organizací. Poskytovatelé těchto specializovaných výpočetních služeb mohou využívat úspor vyplývajících z jejich škálovatelnosti a tak dosáhnout úrovně výpočetních zdrojů nedosažitelné prostřednictvím tradičních přístupů. Cloud computing lze chápat jako prostředek k poskytování výpočetních zdrojů prostřednictvím obdobného modelu jako u elektrických rozvodných sítí a telekomunikačních sítí.

Za zvláštní zmínku z hlediska zaměření tohoto příspěvku stojí, že uživatel služeb cloud computingu nemusí mít žádné znalosti o povaze, lokalitě nebo dokonce vlastnictví souvisejícího hardwaru, tak jako my obvykle neznáme elektrárnu, která přivádí elektřinu do našich domovů.

“Cloud“ je z tohoto pohledu abstrahovaný zdroj softwaru a služeb poskytovaný třetími stranami, k nimž mohou organizace či fyzické osoby přistupovat vzdáleně. Ve své idealizované podobě je uživatel služby cloud computingu oddělen od obav, kde a jak jsou alokovány potřebné prostředky; všechny akce probíhají automaticky prostřednictvím standardizovaných rozhraní, která poskytují požadované služby kdy je jich třeba a jak je jich třeba. V praxi může být realizace tohoto snu složitější a, jak popíší v tomto příspěvku, má svůj vlastní okruh problémů a starostí.

1.1 Modely cloud computingu

Existuje celá řada všeobecně přijatých přístupů k realizaci cloud computingu, které odpovídají různým úrovním abstrakce daných použitým virtuálním hardwarem. Tyto přístupy lze aplikovat různým způsobem a budou vhodné pro plnění různých úkolů požadovaných organizacemi.

Přístupy cloud computing sahají od vzdáleného poskytování softwarových aplikací k poskytování přístupu k samotnému virtuálnímu stroji, na něm lze spustit vlastní software či ho kombinovat s celou řadou dalších služeb. V dalším textu příspěvku budou hlavní formy přístupu ke cloud computingu stručně představeny.

1.1.1 Software as a Service

Na své nejvyšší úrovni abstrakce může cloud computing jednoduše sloužit koncovým uživatelům softwarových aplikací běžících na vzdáleném počítači. Interakce s těmito aplikacemi obvykle probíhá přes webový prohlížeč a umožňuje uživatelům přístup k aplikacím z libovolného místa s připojením k Internetu, a to aniž by se na uživateli požadovalo vlastnictví potřebného hardwaru.

Tento přístup se všeobecně označuje jako software jako služba – Software as a Service (SaaS), což je forma cloud computingu, s níž se koncoví uživatelé pravděpodobně budou setkávat nejčastěji a která jimi bude využívána nejvíce. Do určité míry lze použití softwaru jako služby považovat za logické rozšíření stávajících interaktivních webových technologií.

1.1.2 Platform as a Service

Platforma jako služba – Platform as a Service (PaaS) umožňuje vývojářům s nižší úrovní přístupu ke zdrojům cloudu používat komponenty a služby, potřebné pro vytvoření a nasazení softwaru. Rozhraní sloužící k vývoji aplikací umožňují distribuci a škálovatelnost zdrojů, přičemž zároveň abstrahují od nižší úrovně řízení těchto zdrojů.

Tyto technologie jsou zaměřeny na jednoduchý vývoj aplikací v cloudu, kdy byla obětována jistá pružnost použití platformy na úkor pohodlí vývojářů.

1.1.3 Infrastructure as a Service

Infrastruktura jako služba – Infrastructure as a Service (IaaS) poskytuje nejnižší úroveň přístupu ke zdrojům cloud computingu. V rámci tohoto přístupu má klient plný vzdálený přístup k hostovaným virtuálním strojům a může přímo vyvíjet a nasazovat software, a to obdobným způsobem, jako při tradičním vývoji softwaru. Ve skutečnosti tato forma cloud computingu umožňuje klientovi přístup k velkým serverovým farmám, na kterých lze zákaznický software aplikací podle potřeby dynamicky dislokovat.

Jednou z výhod infrastruktury založené na cloudech je, kromě možné úspory nákladů, schopnost cloudu poskytovat dynamické resp. elastické [7] výpočetní zdroje. Virtualizovaná povaha služeb infrastruktury cloudu umožňuje virtuálním serverům, aby byly podle potřeby přidávány či odebírány z klientových zdrojů. Podniky proto potřebují pouze udržovat výpočetní výkon nezbytný v daném okamžiku a nemusí udržovat maximální dostupné kapacity.

Každý z výše popsaných přístupů ke cloud computing poskytuje uživateli různé úrovně výhod, různé možnosti pro poskytovatele a různé starosti týkající se bezpečnosti a soukromí pokud jde o ukládání, sdílení a přístup k osobním údajům uživatelů. V tomto článku jsme se zaměřili na širší okruhu otázek týkajících se ochrany soukromí v rámci různých forem cloud computingu, a zkoumali způsoby, jimiž se organizace snaží využívat výhod tohoto přístupu při zachování soukromí uživatelů.

2 Soukromí

Problematika ochrany osobních údajů je studována z řady pohledů a interpretace tohoto pojmu se podle toho adekvátně liší. V počítačové vědě se velká část výzkumu soukromí vynořila z oblasti počítačové bezpečnosti se zaměřením na řízení přístupu k informacím a nástrojů v této oblasti používaných. Nicméně i v tomto omezeném kontextu je soukromí pojmem, jehož definice není zdaleka akceptovaná. Je proto vhodné formulovat náš konkrétní výklad termínu soukromí předtím, než zahájíme zkoumání jeho důsledků v cloud computingu.

Aniž bychom se snažili předložit formální definici, nahlížíme v tomto příspěvku na soukromí z hlediska informačního sebeurčení [14], se zaměřením na schopnost jedince udržet kontrolu nad daty popisujícími jeho jedinečné identifikační znaky a historii jeho akcí. Tento výklad umožňuje poměrně široký pohled na soukromá data, pohled, který zahrnuje sociální a obchodní vztahy, sled činností zabývajících se samotným individuem i řadou jeho identit, jež individua představují v jejich interakci, a nakonec i bezprostředními osobními vlastnostmi.

Toto vymezení pojmu soukromí se zaměřuje téměř výhradně na jednotlivce. V tomto příspěvku nebudeme brát v úvahu informace, které mohou být považovány za soukromé, s výjimkou jednotlivých interakcí s danou organizací. Pojem soukromých informací by také neměl být zaměňován s důvěrnými informacemi, týkajících se všech forem informací, které si daná entita přeje uchovat v tajnosti bez ohledu na jejich povahu.

Pro účely tohoto konferenčního příspěvku, který se zabývá problémy soukromí v cloud computingu, jde o to, aby měli jedinci možnost kontrolovat data popisující jejich identitu a akce v cloudu. K lepšímu pochopení, jak maximalizovat tuto kontrolu, nyní budeme zkoumat konkrétní rizika ochrany soukromí ohrožující sen o cloud computingu, a hledat způsoby, jakým tato rizika snížit.

3 Důsledky ochrany soukromí v cloud computingu

Většina základních otázek ochrany soukromí v cloud computingu vychází z údajů, které byly uloženy mimo kontrolu jednotlivé organizace. Tento nedostatek přímé kontroly otevírá kanály, jimiž mohou být informace, ať již úmyslně či ne, uvolněny pro třetí osoby.

Významným a méně nápadným aspektem sdílení dat je, že akce uživatele v cloudu lze pozorovat a zaznamenávat libovolnou entitou podílející se na provádění těchto akcí, jako jsou například uživatelův poskytovatel

internetových služeb a poskytovatel služeb cloudu. To má za následek explozi údajů týkajících se subjektu akce v cloudu, různé formy informací, které mohou ještě nějakou dobu přetrvávat v log souborech a záznamech transakcí. V průběhu doby takto uložená data mohou odhalit základní trendy a chování jednotlivců, které mohou být využívány obtížně předvídatelným způsobem.

Aktuální výpočetní postupy typicky ukládají a zpracovávají citlivé údaje o entitě v rámci přímé sféry kontroly. Pro jednotlivce to bude obvykle jeho domácí PC, zatímco pro větší organizace to obvykle budou servery a pracovní stanice fyzicky umístěné v rámci organizace.

To poskytuje organizacím možnost omezit přístup do velmi jasně vymezené zóny důvěry. V cloud computingu, kde skladování a zpracování zákaznických dat se již neprovádí pouze v organizaci, musí být tato zóna důvěry rozšířena na jednu či více třetích stran.

Toto sdílení dat je do značné míry jednosměrný proces. Sdílení dat je nesmírně obtížné a prokazatelným způsobem je nelze vzít zpět. Ať již jsou použita právní, politická či technická řešení, snadnost a nezjistitelnost kopírování dat jedním nebezpečným či nepozorným zaměstnancem mohou vést ke ztrátě dat.

Outsourcing výpočetních zdrojů není určitě nový fenomén. Mnoho jednotlivců a malých podniků hostuje své internetové stránky prostřednictvím specializované třetí strany, malé firmy používají služby třetích stran pro zpracování plateb a sledování objednávek, stále běžnější je vzdálené zálohování a použití systémy pro ukládání dat. Cloud computing se principiálně neliší od těchto již zavedených služeb, nýbrž je dovádí k logickému závěru, v němž je takto poskytována většina služeb, a to i pro významné společnosti.

Dálkové uchovávání zákaznických dat je však z hlediska dopadů na soukromí ta nejjednodušší a nejpatrnější forma použití cloud computingu. Nyní se budeme zabývat složitějšími dopady, které mohou mít postupy cloud computingu na jednotlivce.

3.1 Pozorovatelné aktivity

Domácí uživatel typicky používá software, který je z velké části uložen a zpracováván na lokálním počítači, přístup k Internetu pak používá s cílem získat data a komunikovat s vnějším světem. Bezprostřední činnosti uživatelé nicméně provádí z velké části v rámci lokálního systému, i když vyžadují interakci s Internetem. Editace dokumentů a obrázků, hraní her a poslech hudby stále více a více vyžadují připojení k Internetu. U těchto požadavků jde především o přenos obsahu, přičemž zpracování a uchování probíhá na lokálním počítači.

Cloud computing se snaží prolomit bariéru mezi počítači uživatele a cloudem vzdálených poskytovatelů služeb. Dokumenty, fotografie a videa jsou nejen uchovávány a zpřístupňovány on-line, ale používaný software pro jejich vytváření a editaci je rovněž umístěn a spouštěn vzdáleně.

To přidává další vhodnou vrstvu pro uživatele, kteří již nyní nevyžadují nákup a údržbu výkonných strojů. Nicméně z hlediska soukromí poskytovatel služby cloud computingu nyní získává detailní pohled na činnost uživatele. Poskytovatel už vidí nejen nahrané dokumenty, obrázky a videa, ale je zapojen do všech aspektů procesu jejich tvorby, včetně prvotních návrhů a průběžné editace.

Kromě toho používání profilů a přístupové časy ukazují, kdy uživatel pracoval na dokumentu, kdy se zastavil na jídlo a kdy šel spát. Konferenční příspěvek [17] prokázal, že sledování domácí dodávky elektřiny může odhalit překvapující množství informací týkajících se individuálních zvyků uživatele; když tento postup rozšíříme na podrobné sledování on-line aktivit na Internetu, lze získat množství informací, s jejichž pomocí lze podstatným způsobem zasáhnout do soukromí jednotlivce.

3.2 Pozorovatelné interakce

Zvýšená kontrola uživatelských aktivit poskytovatelem cloudu může způsobit v oblasti soukromí vážná rizika. Z vnějšího pohledu dokonce i uživatelské vztahy s různými službami cloudu o něm mohou pozorovateli potenciálně poskytnout spoustu informací.

V cloud computingu uživatelé rozvíjí stále větší počet kritických vztahů s poskytovateli služeb, kteří je krmí množstvím informací nebo zábavy, ale také narůstají relace se softwarem, který uživatelé potřebují pro svůj každodenní život. Tento software není, jak je tomu u tradičního modelu, stahován na lokální počítač a pak spouštěn, nýbrž se opírá o konstantní interakce mezi poskytovatelem a spotřebitelem.

Důsledkem toho, že nejen data, ale i software je umístěn vzdáleně, je, že pozorovatel toku dat provozu k počítači a od něj může shromažďovat informace o typu softwaru nainstalovaném na počítači uživatele a kdy je tento

software zpřístupňován. I když tato informace nemusí být vždy rozhodující, znalost interakce uživatele s lékařskou či finanční službou lze považovat za závažné porušení soukromí.

3.3 Agregace služeb

V případě použití služby cloud computingu koncový uživatel akceptuje, že jeho zákaznické informace a data jsou uloženy na systému poskytovatele služeb. Uživatel rovněž akceptuje to, že poskytovatel služeb získá podrobnější přehled o jeho činnosti a zvycích, a že pozorovatel se schopností monitorovat jeho připojení k Internetu má možnost zjistit některé aspekty jeho chování.

U poskytovatele služeb je nepravděpodobné, že by poskytoval pouze jedinou službu nebo produkt. Větší poskytovatelé nabízejí celé sady softwaru, které spouštějí vzájemně propojené úlohy využívající různý software. Z hlediska interoperability je zřejmě lépe volit použití produktu jediného poskytovatele, než si vybírat z celé řady konkurenčních produktů.

Když uživatel používá celou škálu softwaru od jediného poskytovatele služeb, ten tím získává informace nejen o jeho aktivitách z hlediska jedné aplikace, ale z hlediska celé sady aplikací. Jak již to bývá v oblasti ochrany soukromí, hodnota těchto souhrnných údajů je podstatně vyšší, než součet hodnot jeho částí.

3.4 Agregace infrastruktury

Agregace služeb umožňuje poskytovateli softwaru cloudu monitorovat uživatelův přístup k datům a zjišťovat charakter používání celého spektra poskytovaných služeb a tím potenciálně odhalit mnohem větší množství informací, než by uživatel čekal. Toto riziko může být dokonce ještě vyšší, pokud velké entity cloud computingu nebudou vystupovat vůči uživateli jako poskytovatelé softwaru pro uživatele, ale jako poskytovatelé zdrojů pro organizace.

Model infrastruktury jako služby je navržen tak, aby umožnil organizacím přímý přístup k výpočetním službám nízké úrovně, jako jsou virtuální stroje [11]. Ty mohou být organizacemi použity k vytváření vlastní softwarové služby, včetně aplikací cloudu vyšší úrovně.

V tomto scénáři jsou poskytovatelé infrastruktury schopni sledovat chování zákazníků těchto organizací, které budou vycházet z jejich infrastruktury. Tito zákazníci si obvykle nejsou vědomi toho, že se pod jim poskytovanými službami skrývají poskytovatelé infrastruktury, ani že s nimi nemají přímý právní vztah. Zvláštní obavy v tomto scénáři vzbuzuje, že při individuálním přístupu zabezpečeném dvěma zcela samostatnými poskytovateli aplikace cloudu lze nevědomky komunikovat přes infrastrukturu cloudu, která má stejného poskytovatele.

Osobní údaje zákazníků budou v těchto scénářích téměř jistě chráněny dohodou o úrovni služby a není pravděpodobné, že by poskytovatel infrastruktury měl povolení, aby tyto údaje použil. Navzdory tomu jak agregace služeb, tak agregace infrastruktury vytváří centralizovaný bod pro pozorování a sledování uživatelů, který tak poskytuje lákavý cíl pro hackery či prostě pro nedůvěryhodné zaměstnance snažící se shromažďovat velké množství privátních informací.

3.5 Ekonomika osobních informací

Model výpočtu jako služby je atraktivní v mnoha ohledech, s významnými výhodami pro spotřebitele i poskytovatele. Protože jde o logické rozšíření stávajících internetových služeb, je pravděpodobné, že se někteří poskytovatelé služeb rozhodnou, že tyto služby nebudou uživatelům účtovat přímo, ale místo toho budou odvozovat zisk z cílené reklamy a prodeje údajů o zákaznících.

Zacházení s osobními údaji jako jisté „platidlo“ za přístup ke službám je lákavé jak pro koncové uživatele, kteří obvykle mívají relativně malé obavy o narušení svého soukromí, tak pro poskytovatele, kteří těží ze zdánlivě „zdarma“ služeb.

Jedním ze znepokojujících výsledků tohoto trendu je, že uživatelé, kteří jsou si vědomi rizik z hlediska narušení soukromí, si mohou velmi obtížně volit některou z populárních služeb, které od nich vyžadují, aby předložili své osobní údaje. Pokud se určité služby stanou téměř univerzálními, tito uživatelé mohou mít komunikační problémy v podnikání či osobním životě, budou-li chtít používat služby z kategorie kancelářského softwaru a sociální sítě. Cloud computing může zhoršit tuto situaci tím, že promítne platby prostřednictvím osobních informací mnohem hlouběji do života uživatelů.

Tyto přirozené monopoly mohou být sníženy podporou otevřených standardů softwaru, které umožňují interoperabilitu mezi různými službami a poskytovateli, a tak vytvářejí tržní alternativu jakémukoliv danému produktu. Bohužel, toto není obvykle považováno za záležitost v nejlépeším zájmu poskytovatelů služeb. Historie ukázala, že mnoho velkých poskytovatelů softwaru dává přednost zachování svého vlastního proprietárního přístupu.

3.6 Požadovaná participace

Zatímco vyhýbání se dominantním produktům se může ukázat jako velmi nepohodlné, existují služby, jimž se nedá vyhnout vůbec. To platí zejména o vládních službách, které také mohou být hlavním úložištěm vysoce citlivých osobních informací.

Pokud se vlády rozhodnou outsourcovat své infrastruktury do cloudu, jsou s tím spojené otázky soukromí a bezpečnostní rizika předány do rukou civilistů. A přitom je jasné, že služby na úrovni vlády jsou obzvláště lákavým cílem pro hackery, a to vzhledem k významu informací, které jsou v nich uloženy.

Poskytovatelé cloud computingu používaného pro vládní služby musejí očekávat, že tak jako všechen software a hardware používaný vládou i cloudy budou muset splňovat přísná kritéria z hlediska bezpečnosti a soukromí. Vývoj takovýchto kritérií musí vzít v úvahu nejen informace uložené v systému, ale i jejich interaktivní způsob chování v cloudu.

4 Bezpečnost cloudu

Jednou ze základních změn, jimiž cloud computing prochází, je software poskytovatelem cloudu kompletně nainstalovaný na jeho systémy, bez toho, že by se spoléhalo na méně zkušené domácí uživatele. I když, jak již bylo diskutováno, to odhaluje poskytovateli mnohem víc o používání počítačů a obsahu osobních údajů, na druhé straně je zde možnost snížit rizika ze špatně nakonfigurovaného či nechráněného softwaru běžícího na počítači uživatele. Zatímco viry, trojské koně a spyware jsou nadále možné i v cloud computingu, tyto hrozby se posouvají spíše směrem k poskytovatelům než ke koncovým uživatelům.

Nejvýznamnějším negativním aspektem tohoto spoléhání se na software na straně serveru je, že jakékoli porušení software poskytovatele odhalí obrovské množství osobních informací. Je tudíž možné, že až se cloud computing více rozšíří, dojde k narušení soukromí sice méně často, ale bude mít dramatičtější důsledky.

5 Specifické problémy modelu

V předchozí části příspěvku jsme se zabývali dopady cloud computingu na soukromí v širším kontextu. Nyní se budeme krátce zabývat obavami o zachování soukromí, které vznikají u každého z hlavních přístupů k cloud computingu.

5.1 Software as a Service

Software jako služba je z hlediska koncového uživatele nejviditelnější formou cloud computingu, protože poskytuje přímý přístup k softwarové aplikaci v cloudu. Toto řešení má potenciál alespoň částečně nahradit stávající uživatelský model, kdy mají uživatelé software nainstalován na svém stroji ve prospěch připojení ke vzdálené aplikaci.

Uživatelé mají v tomto modelu jen malou možnost zkontrolovat, jak jsou jejich informace v rámci platné politiky ochrany osobních údajů uloženy a sdíleny poskytovateli. Dodržování těchto norem totiž může být velmi obtížně ověřitelné, protože únik soukromých informací je zřídka zjistitelný. Přesto uživatelé on-line služeb v posledních letech projevili rostoucí zájem o dobře navržené politiky ochrany soukromí. Protesty uživatelů měly dostatečně silný vliv na změny v politice velkých organizací.

Povaha tohoto modelu poskytování softwaru a relativní nedostatek síly a kontroly, že uživatelé dostatečně ovládají software poskytovatele, vyžadují vysoký stupeň důvěry ze strany uživatelů. K tomu, aby tato důvěra byla nějakým způsobem odůvodněná, je třeba, aby byly rozvíjeny mechanismy pro zajištění souladu s politikami a právními mechanismy, a to spolu se silnými podněty pro interoperabilitu softwaru, aby bylo zabráněno zablokování uživatele.

5.2 Platform as a Service

Platforma jako služba systému umožňuje zákazníkům vyvíjet software cloud computingu na vysoké úrovni abstrakce, aniž by bylo potřebné mít přístup k detailům infrastruktury.

Tento model představuje pro vývojáře zajímavý soubor konstrukčních problémů týkajících se oblasti soukromí. Největší obavy v tomto modelu vzbuzuje, že podrobnosti nízké úrovně, tj. kde a jak jsou uloženy informace, jsou abstrahovány mimo přímou kontrolu vývojáře, a pak může ve svém kódu nízké úrovně, na kterém je postaven software, nechat díry, jimiž mohou unikat informace narušující bezpečnost či soukromí uživatelů. To může mít podobu zbytečné či pozorovatelné komunikace mezi hostiteli, nebo nezabezpečeného skladování resp. replikací dat.

Při vývoji software na této úrovni by měla být nejdůležitější zásadou minimalizace dat [13], podle které by měla být soukromá data ukládána pouze tehdy, pouze pokud to je absolutně nezbytné. Tím, že se odstraní zbytečné informace, může vývojář výrazně zmírnit nepředvídatelné riziko. I když tento přístup by měl být považován při návrhu softwaru zpracovávajícího soukromé informace za zásadní, nedostatek přímé kontroly nad použitými mechanismy činí tuto záležitost obzvláště kritickým faktorem.

5.3 Infrastructure as a Service

Infrastruktura jako služba je pro běžné uživatele cloud computingu do značné míry něčím neviditelným. Protože má vývojář přímý přístup k detailům infrastruktury nízké úrovně, v tomto modelu cloud computingu získává detailní kontrolu nad mnoha aspekty toho, jak jsou data přenášena a ukládána. To poskytuje možnost větší pružnosti při navrhování aplikací a architektur se vztahem k soukromí.

Nehledě na tyto možnosti infrastruktura jako služba nutně nemusí vývojáři poskytovat plnou kontrolu nad umístěním svých zdrojů ani konkrétní podrobnosti o tom, jak jsou přidělovány virtuální prostředky. Stejně jako u všech přístupů ke cloud computing, jsou prostředky alokovány třetí stranou, která má plný přístup ke všem údajům a výpočet provádí jako službu. To ponechává konečnou odpovědnost za bezpečnost dat, a tedy i za ochranu osobních údajů, na poskytovateli příslušného cloudu.

6 Právní úvahy

Tento konferenční příspěvek se zaměřuje především na technické aspekty ochrany soukromí v cloud computingu, ovšem bylo by chybou ignorovat celou škálu právních otázek, jakož i příslušné právní ochrany, které souvisí s cloud computingem. Na tomto místě se jim proto budeme stručně věnovat.

Individuální právo na soukromí je celosvětově široce uznáváno a je Organizací spojených národů zakotveno ve Všeobecnou deklaraci lidských práv [10]. Zvláštní pozornost, kterou dnes právo věnuje soukromí, je v mnoha západních zemích poměrně čerstvá záležitost [18] a jeho konkrétní použití ještě bude předmětem řady debat.

Interakce mezi velkou částí globálního Internetu a místními zákony je věčným zdrojem obav z nových technologií a cloud computing jistě není žádnou výjimkou z tohoto pravidla.

Snad nejvýznamnějším problémem práva s cloud computingem je to, že soukromá data vstupující do cloudu mají schopnost přecházet mezi různými jurisdikcemi, které představují diametrálně odlišné úrovně ochrany soukromí. Tak tomu může být i v případě, kdy abstrakce výpočetních zdrojů umožňuje technologii cloudu, aby vývojář nevěděl, kde data shromážděná pro jeho použití mohou být skladována. V případě evropských zákonů na téma soukromí, které stanovují, že soukromé informace nemohou být předávány do zemí s neslučitelnými zákony na ochranu soukromí, může mít aplikace cloud computingu velké potíže při plnění svých zákonných povinností [16].

Právní mechanismy jsou tudíž rozhodující překážkou tomu, aby služby cloudu fungovaly efektivně. Dále musí být tyto mechanismy vyvinuty společně s technologií cloudu a musí samy o sobě být vytvářeny s cílem poskytovat odpovídající rámec, v němž tyto technologie mohly efektivně fungovat.

7 Řešení ochrany osobních údajů

Nyní stručně prozkoumáme principy a techniky, které mohou být použity na zmírnění problémů ochrany soukromí v cloud computingu.

Základním principem ochrany osobních údajů, a pravděpodobně nejvíce efektivním, je minimalizace; údaje by neměly být sbírány, skladovány, nebo sdíleny, pokud to není pro fungování služby nezbytně nutné. Bylo opakovaně prokázáno [6] [9], že i zdánlivě triviální ukládání dat může mít za následek vážné narušení soukromí, když jsou údaje agregovány a analyzovány.

Druhou zásadou, která je klíčem k uchování soukromí v cloud computingu, je, že jakmile byla data sdílena s třetí osobou, nelze je snadno udržet v tajnosti. Zákony a zásady ochrany osobních údajů, které na poskytovatelích požadují, aby osobní data po určité době vymazali, poskytují užitečný návod, a umožňují, aby byly organizace potrestány, pokud s daty není nakládáno patřičným způsobem; nicméně tyto metody mohou být aplikovány pouze tehdy, když ke sdílení dat skutečně došlo a zároveň, když bylo toto sdílení zjištěno.

Na druhé straně technická řešení mají za cíl zabránit možnosti neoprávněného sdílení dat. Škála technologií, které máme k dispozici, poskytuje sama o sobě silné záruky, že data nemohou být zneužita. Bohužel, mnohé teoretické techniky jsou křehké, nepohodlné, výpočetně náročné a obtížně implementovatelné do fungující služby.

7.1 Homomorfní šifrování

Šifrování – matematické transformace informací s cílem znemožnit čtení textu kýmkoliv, kdo nezná utajovaný klíč – je základním stavebním kamenem moderního Internetu. Šifrování se používá při přenosu dat, zatímco v cloud computingu má jen omezené využití pro takové účely, jako je ukládání statické informace.

V roce 2009 Craig Gentry navrhl plně homomorfní šifrovací systém [4] ve snaze vyřešit dlouhotrvající zásadní výzvu moderní kryptografie. Gentryho schéma získalo velkou pozornost jako řešení široké škály problémů v oblasti bezpečnosti a ochrany soukromí. My se zde budeme stručně zabývat jeho možnostmi a omezeními.

Jednoduše řečeno, plně homomorfní šifrovací schéma umožňuje třetí straně, jako je poskytovatel cloud computingu, provádět libovolné operace na šifrovaných datech bez nutnosti tato data dešifrovat. Výhody tohoto schématu pro cloud computing jsou evidentní: s třetí stranou může být uzavřena smlouva na zpracování dat pro zákazníka bez toho, aby tato třetí strana znala jejich obsah. To je velkou výhodou pro podniky, které velmi neochotně sdílejí své citlivé duševní vlastnictví s třetími stranami.

Homomorfní šifrování není v žádném případě univerzálním řešením pro ochranu soukromí uživatelů. I za předpokladu, že se takovýto systém stane prakticky použitelný, a to na rozdíl od dosud nejnámějšího přístupu, který je o několik řádů pro reálné použití neefektivnější, homomorfní šifrování řeší pouze jeden z mnoha způsobů, jimiž mohou být soukromé informace uživatelů ohroženy.

Jak je podrobně uvedeno výše, soukromí uživatelů přesahuje obsah zákaznických databází a vzdáleného zálohování. Šifrování obsahu stále ještě umožňuje jak pozorovatelům, tak poskytovatelům cloudu učit se znát komunikační partnery, historii transakcí, uživatelské profily a mnoho dalších aspektů akcí uživatelů [19]. Homomorfní šifrování tudíž v případě, že se někdy stane praktickou technologií, bude stejně jen jednou částí širšího přístupu k ochraně soukromí v cloudu.

Kromě různých forem šifrování dat, služby cloud computingu, vysoce citlivé z hlediska soukromí, mohou rovněž využít výhod celé škály výsledků současného vývoje kryptografického výzkumu, jako jsou anonymizované komunikační systémy [1], [2], [3], skrývající vztahy mezi spotřebiteli a poskytovateli; systémy vyhledávání soukromých informací [12], které umožňují klientům získávat informace z databáze, aniž by vlastník databáze mohl určit, které záznamy byly zpřístupněny; a mnohostranné výpočty, které umožňují klientům rozestřít výpočetní zdroje mezi zařízení více poskytovatelů tak, aby se žádný z nich nedozvěděl detaily toho, co bylo vlastně zpracováno [5]. Tyto technologie jsou sice v současnosti z větší části teoretické konstrukce, ale nároky na cloud computing mohou vést k jejich rostoucímu využití v praxi.

8 Závěr

Cloud computing je vzrušující technologie, která koncovým uživatelům poskytuje řadu praktických výhod; pro velké podniky platí totéž. Rostoucí trend směrem k vzdáleně hostovaným službám znamená, že cloud computing bude pravděpodobně v budoucnosti výpočetní techniky hrát velkou roli, ale jak již to bývá u každé nové technologie, její finální podoba se od té aktuální bude zřejmě značně lišit.

Nicméně i přes své výhody cloud computing budí značné množství velmi vážných obav o soukromí. Nejzřejmější z těchto obav je dálkové ukládání dat, ale, jak jsme popsali, existuje mnoho dalších. Sdílení dat s třetími stranami

je skutečně v protikladu se soukromím, a podniky, které nahlíží na osobní informace jako na zdroj příjmů, je soukromí ohroženo dokonce ještě více.

Dále je nepravděpodobné, že v dlouhodobém horizontu cloud computingu zanecháme. Z obchodního a vládního hlediska budou naopak poskytovatelé našich služeb této technologie využívat stále více, a to na všech úrovních. Proto je tak důležité, aby technologie ochrany dat zaměřené na cloud computing byly vyvíjeny souběžně s dalšími technologiemi cloud computingu a byly rovněž považovány za fundamentální součásti jejich návrhů.

Z uživatelského pohledu je důležité, že minimalizujeme množství poskytovaných informací. Na základě existujících příkladů z oblasti síťových služeb můžeme považovat za vysoce nepravděpodobné, že uživatelé budou soukromí považovat za dostatečně důležitý faktor pro vyvážení se z pohodlných služeb. Musí tedy existovat právní požadavky na poskytovatele cloudu s cílem zajistit dostatečně přísné politiky pro jejich služby, které musí být podpořeny potřebnými mechanismy, jakož i prostředky k zajištění uplatňování příslušných zákonů.

Cloud computing nabízí mnoho příležitostí a mnoho rizik, přičemž veškeré důsledky této technologie je těžké předvídat. Důležité však je, že úvahy o významu soukromí vznikají již při zrodu této technologie, než aby byly zanedbávány v době, kdy tato technologie zraje. Tímto způsobem pocítí výhody cloud computingu nejen podniky a podnikatelé, ale i běžní uživatelé, kteří s těmito technologiemi přijdou do styku.

Použité zdroje

- [1] Jan Camenisch and Els Van Herreweghen. Design and implementation of the idemix anonymous credential system. In CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, pages 21–30, New York, NY, USA, 2002. ACM.
- [2] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 4(2), February 1981.
- [3] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In Proceedings of the 13th USENIX Security Symposium, August 2004.
- [4] Craig Gentry. Fully homomorphic encryption using ideal lattices. In STOC, pages 169–178, 2009.
- [5] Oded Goldreich. Secure multi-party computation. Working Draft, 2000.
- [6] Philippe Golle. Revisiting the uniqueness of simple demographics in the us population. In WPES'06: Proceedings of the 5th ACM workshop on Privacy in electronic society, pages 77–80, New York, NY, USA, 2006. ACM.
- [7] Amazon Inc. Amazon Elastic Compute Cloud (Amazon EC2). Amazon Inc., <http://aws.amazon.com/ec2/>, 2008.
- [8] Peter Mell and Tim Grance. The nist definition of cloud computing. Technical report, National Institute of Standards and Technology, Information Technology Laboratory, July 2009.
- [9] Arvind Narayanan and Vitaly Shmatikov. How to break anonymity of the netix prize dataset. CoRR, abs/cs/0610105, 2006.
- [10] United Nations. Universal declaration of human rights. Australian National Committee for United Nations, Melbourne , 1949.
- [11] Daniel Nurmi, Rich Wolski, Chris Grzegorzczak, Graziano Obertelli, Sunil Soman, Lamia Youseff and Dmitrii Zagorodnov. The eucalyptus open-source cloud-computing system. In Proceedings of Cloud Computing and Its Applications, October 2008.
- [12] Rafail Ostrovsky and William E. Skeith III. A survey of single-database private information retrieval: Techniques and applications. In *Public Key Cryptography*, pages 393–411, 2007.
- [13] Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, December 2009. v0.32.
- [14] Gebhard M. Rehm. Just Judicial Activism? Privacy and Informational Self-Determination in U.S. and German Constitutional Law. SSRN eLibrary, 2000.
- [15] E. Eugene Schultz. A futuristic look at cloud computing security. Forthcoming. (2010 Information

Security Summit, Prague.), 2010.

- [16] Staff. Eu assesses adequacy of us safe harbor privacy compliance. *IWAYS*, 28(1):27–33, 2005.
- [17] M. Stringer, G. Fitzpatrick, D. Chalmers, E. Harris, R. Krishna, and M. Haarlander. Kuckuck exploring ways of sensing and displaying energy consumption information in the home. In *Proceedings of Workshop on Ubiquitous Sustainability: Technologies for Green Values (at UbiComp 2007)*, 2007.
- [18] Samuel D. Warren and Louis D. Brandeis. The right to privacy. *Harvard Law Review*, 4(5):193–220, December 1890.
- [19] Whitfield Diffie, Susan Landau. Privacy on the line: the politics of wiretapping and encryption. *SIGACT News* 39(4): 30–32 (2008).

