Bezpečnosť cloudových riešení so zameraním na mobilné aplikácie

Mária Szivósová[1]

Abstrakt
Cieľom článku je analyzovať bezpečnostné prvky cloud computingu a takisto analyzovať využívanie týchto služieb v mobilných zariadeniach. V článku sme definovali jednotlivé bezpečnostné prvky využívane v informačno-komunikačných technológiách na základe ktorých sme rozpracovali detailné analýzy troch najväčších hráčov v tomto priemysle. Výsledkom týchto analýz je tabuľka, ktorá porovnáva jednotlivé bezpečnostné opatrenia. Z tejto tabuľky je vidieť, že títo poskytovatelia berú bezpečnosť vážne a disponujú kvalitným zabezpečeným. Je zrejmé, že medzi nimi prebieha konkurenčná hra a snažia sa získať zákazníka na svoju stranu. Preto sa snažia stále zlepšovať. Myslíme si, že technológia cloud computingu by mala mať väčšiu popularitu v širšej verejnosti. Prechod na cloud by zefektívnil činnosti rôznych podnikov a organizácií za nižšie náklady ako je to pri tradičnej počítačovej infraštruktúre. Na druhej strane by si mal byť každý vedomí, že ku cloudom sa pristupuje prostredníctvom internetovej komunikácie a s ňou sú spojené rôzne bezpečnostné hrozby. Rôzne verejné hotspoty môžu byť nezabezpečené, a tým vystavujeme naše mobilné zariadenia nebezpečenstvu. Kvalitné poznatky ohľadom bezpečnosti informačných systémov a technológii, môžu byť kľúčové pri snahách o bezpečný prechod do prostredia cloudu.

Kľúčové slová
cloud computing, bezpečnosť, mobilný cloud computing, mobilné zariadenie, zdieľanie výpočtových prostriedkov, poskytovateľ služby

Abstract
The aim of the article was to analyze the security features of cloud computing, and also to analyze the use of these services on mobile devices. In the article we defined the various security elements used in information and communication technologies on which we developed detailed analyzes of the three largest players in the industry. Results of these analyzes is a table that compares the different security measures. This table shows that these providers take security seriously and is very well secured. It is obvious that between them runs a competitive game and try to get customers to your side. That is why we constantly improve.We think that cloud computing should be more popular in the wider community. The transition to cloud to streamline the activities of various companies and organizations at a lower cost than is the case in traditional computing infrastructures. On the other hand, you should be aware of all that to the cloud are accessed through Internet communication and with it are connected to various security threats. Various public hotspots can be insecure and thus expose our mobile safety. Quality knowledge about security of information systems and technology, could be essential in efforts to secure the transition to the cloud.

Key words
cloud computing, security, mobile, cloud computing, mobile devices, sharing computing resources, services agreement

JEL classification
M15

[1]University of Economics in Bratislava, Faculty of Economic Informatics, Department of Applied Informatics, Dolnozemská cesta 1, 852 35 Bratisava, e-mail: maria.szivosova@euba.sk

1 Úvod

Koncom 20. storočia nastal obrovský progres v rozvoji informačno-komunikačných technológií a internetu. Jednotlivé firmy aj domácnosti začali používať moderné technológie, ktoré im umožňujú efektívne spracovávanie a ukladanie dôležitých dát. Prinieslo to takisto aj negatíva v podobe zlého zabezpečenia dát, krádeži dát, zneužitia dát a iných hrozieb. Vzrástli požiadavky na lepšie zabezpečenie, rýchlosť prenosu, kapacity ukladania dát a mobilitu dát. 21. storočie prinieslo nový pojem z oblasti informačno-komunikačných technológií - cloud computing.

Cloudové riešenia a ich bezpečnosť so zameraním na mobilné aplikácie, ktoré ozrejmujeme v článku, je ako téma veľmi aktuálna, z dôvodu veľkého potenciálu tejto technológie v budúcnosti. Veľa ľudí denne využíva tieto cloudové služby a ani o tom nevie. Chceli by sme objasniť pojem cloud computing, jeho bezpečnosť a využitie aj na mobilných zariadeniach. Práve tieto atribúty sú dnes najviac žiadané, ale relatívne slabá znalosť verejnosti spomaľuje rozvoj tohto fenoménu.

2 Od distribúcie výpočtových prostriedkov po informačno-komunikačné technológie

Myšlienka distribúcie výpočtových prostriedkov vznikla už v 60. rokoch 20. storočia, kedy sa obor IT iba rozbiehal. John McCarthy v roku 1961 predvídal, keď vyhlásil, že „jedného dňa budú výpočtové prostriedky dostupné ako verejná služba“ (Antonopoulos, Nick - Gillam, Lee, 2010), podobne je tomu napríklad pri distribúcii elektrickej energie, zemného plynu alebo vody. Za prvú realizáciou tohto konceptu v praxi považujeme prenájom strojového času ponúkaný vybraným zákazníkom firmou IBM prostredníctvom operačného systému TSS/360 určeného pre mainframe platformu IBM System/360.(Pugh, Emerson W. – Johnson, L. R. 1991)

Na myšlienky Johna McCarthyho v roku 1966 nadviazal Douglas F. Parkhill vo svojom diele „The Challenge of the Computer Utility“. Jeho definícia sa už podobá na dnešnú podobu cloudu, teda funguje ako on-line dostupná verejná služba.(Parkhill, D. F. 1966) V roku 1969 sa zrodila myšlienka „intergalaktickej počítačovej siete“ alebo „galaktickej siete“ (koncept podobný dnešnému internetu). Rodičom tejto myšlienky bol J.C.R. Licklider, ktorý bol zodpovedný za umožnenie rozvoja ARPANETu (Advanced Reaserch Project Agency Network). Jeho víziou bolo spojiť všetkých na svete tak, aby mali prístup k programom a dátam v akomkoľvek mieste a odkiaľkoľvek.(Naumann, F. 2009)

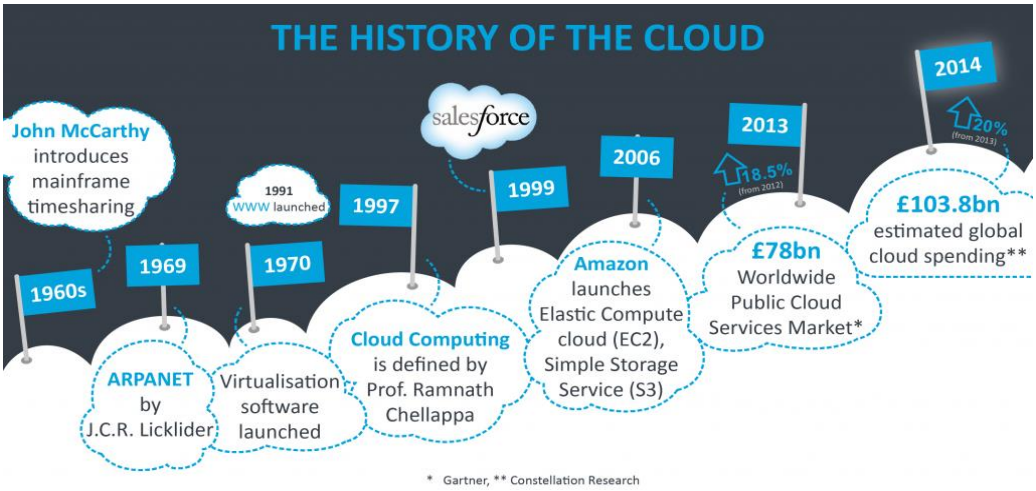
V roku 1970 sa začal používať virtualizačný software VMware, kde bolo možné spustiť viac ako jeden operačný systém súčasné v izolovanom prostredí. Dal sa spustiť úplné iný počítač vo vnútri iného operačného systému.

Samotný výraz „cloud computing“ však vznikol podstatne neskôr. Prvý krát bol použitý až koncom 90. rokov 20. storočia. Prvý krát bolo toto slovné spojenie vyslovené v univerzitnom prostredí Ramnathom Chellappovom, ktorý ho v roku 1997 použil na svojej prednáške na konferencii INFORMS v Dallase, USA.(Chellappa, R. 2012) Tento termín spopularizovali až veľké IT firmy, ktoré sa dajú nazvať priekupníkmi moderného cloud computingu, najmä Amazon, Microsoft, Google alebo IBM. Dôležitú úlohu vo vývoji cloudu zohrala firma Amazon, ktoré prostredníctvom modernizácie dátových centier, ktoré používali iba 10% svojej kapacity a to kvôli ponechaniu si priestoru pre budúce príležitosti. Zistilo sa, že nová architektúra zlepšila vnútornú efektivitu. Amazon poskytuje od roku 2006 prístup k svojim systémom prostredníctvom Amazon Web Services.

Od roku 2008 toto IT odvetvie zaznamenáva prudký rast, čomu napomohla aj ekonomická kríza. Prenájom služieb z cloudu firmám znižuje náklady súvisiace s IT infraštruktúrou. V roku

2013 celosvetový trh verejnej cloudovej služby vyhodnotil na 110 miliárd USD, s architektúrou IaaS (infastructure-as-a-service) zaznamenal rast oproti roku 2012 o 18,5%. Analytická spoločnosť Forrester podľa posledného prieskumu predpovedá, že objem trhu bude ďalej rasť až na 241 miliárd USD v roku 2020. (Ried, S. – Kisker, H.,2011).

Obr. 1: Vývoj cloud computingu



Zdroj: http://timesofcloud.com/cloud-tutorial/history-and-vision-of-cloud-computing/

2.1 Definícia pojmu a hlavné charakteristiky cloud computingu

Cloud computing je model umožňujúci pohodlný, sieťový prístup na vyžiadanie do zdieľanej pamäte konfigurovateľných výpočtových zdrojov (napr. siete, servery, úložné zariadenia, aplikácie a služby), ktoré možno rýchlo zásobiť a uvoľniť s minimálnym manažérskym úsilím a riadením alebo interakciou s poskytovateľom služieb. Tento cloud model podporuje dostupnosť a skladá sa z päť základných charakteristík, troch distribučných modelov a štyroch modelov nasadenia. podľa: NIST (National Institute of Standards and Technology)

NIST (National Institute of Standards and Technology) definoval aj týchto 5 charakteristík cloud computingu:

On-demand self-service (Samoobsluha na vyžiadanie)

Pre tento princíp je kľúčové, že „zákazník môže samostatne získať výpočtové zdroje, časový server alebo úložný priestor pre dáta podľa vlastnej potreby bez nutnosti komunikácie s poskytovateľom požadovanej služby[8] V porovnaní s tradičnou výpočtovou technikou tento princíp ponúka vyššiu úroveň flexibility poskytovaných služieb, teda schopnosť rýchlej reakcie na zmenu požiadaviek kladených na rozsah a úroveň požadovaných výpočtových prostriedkov.

Broad network access (širokopásmový prístup po sieti)

Ďalšou základnou vlastnosťou je požiadavka na využitie „širokopásmového prístupu po sieti prostredníctvom štandardných mechanizmov, ktoré umožňujú pripojenie heterogénnych tzv. tenkých alebo tlstých klientov (mobilné telefóny, tablety, notebooky, stolné počítače atď.).“ (Mell, P. - Grance, T. 2011) Toto úzko súvisí s problémom dostupnosti dát v cloude.

Resource pooling (zlučovanie prostriedkov)

Princíp zlučovania prostriedkov je zobrazený z pohľadu poskytovateľa cloudových služieb. „Výpočtové prostriedky poskytovateľa sú zlučované takým spôsobom, aby mohli byť v zdieľanom prostredí dynamicky poskytované či odoberané rôznym zákazníkom na základe

ich požiadaviek“[8] S tým súvisí problém dostupnosti a bezpečnosti dát – zákazník nemá bežne možnosť ovplyvniť ani zistiť, kde sa nachádzajú zdieľané výpočtové prostriedky.

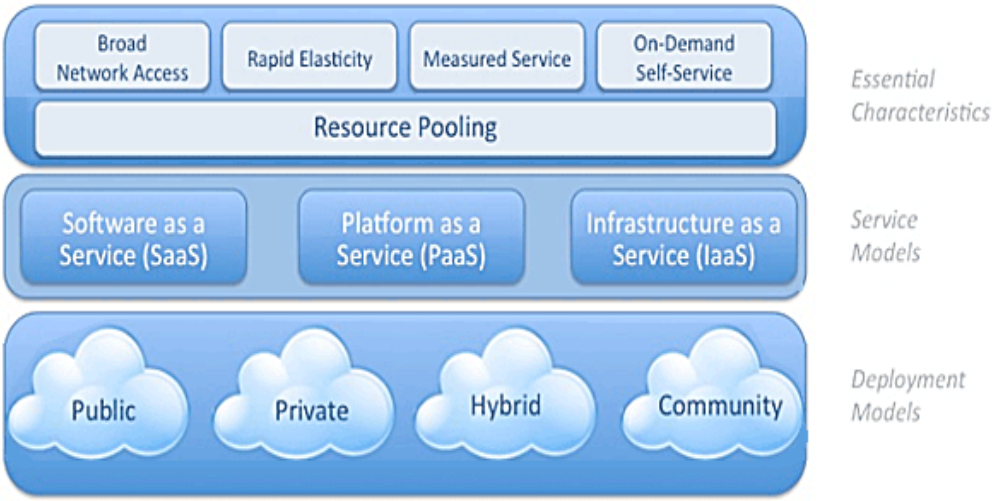
Rapid elasticity (rapídna elasticita)

„Rapídna elasticita“ je podľa odborníkov požiadavka kladená na služby v cloude spočívajúca v možnosti „pružne prideľovať a odoberať výpočtové zdroje v závislosti na ich vonkajšom a vnútornom dopyte. Z hľadiska spotrebiteľa sa poskytované zdroje zdajú byť neobmedzené – môžu byť prideľované v akomkoľvek množstve a kedykoľvek“ (Mell, P. - Grance, T. 2011) „Rapid elasticity“ má tiež kladný dopad na celkovú flexibilitu cloudových služieb.

Measured service (merateľnosť služby)

Princíp merateľnosti služieb poskytovaných zákazníkom je zásadným predpokladom k vytvoreniu ekonomického modelu, v ktorom je užívateľom účtovaná čiastka na základe skutočnej spotreby poskytovaných zdrojov (platobný model označovaný ako „pay-per-use“ alebo „charge-per-use“). „Monitoring, kontrola a reportovanie výpočtových zdrojov umožňuje poskytovateľovi a jeho zákazníkom transparentný prehľad o využití týchto zdrojov“ (Mell, P. - Grance, T. 2011)

Obr. 2: Prvky cloudového modelu



Zdroj: https://www.secureworldexpo.com/cloud-security-prescriptive-approach

IT špecialisti a softvéroví developeri však môžu mať inú predstavu ohľadom cloudu, ako je tu popísaná z pohľadu koncového užívateľa.

2.2 Rozdelenie cloud computingu

Aby sme lepšie porozumeli cloud computingu, musíme definovať jednotlivé typy cloudu. Cloud copmputing môžeme rozdeliť do dvoch odlišných skupín modelov:

- **Modely nasadenia** – týkajú sa umiestnenia a riadenia infraštruktúry cloudu
- **Distribučné modely** – skladajú sa z jednotlivých typov služieb, pomocou ktorých je možné získať prístup k platforme

Modely nasadenia

Cloud computing sa podľa NIST delí na verejný, súkromný, hybridný a komunitný cloud.

Verejný cloud

Verejná cloudová infraštruktúra je k dispozícií na verejné použitie alebo pre veľké priemyselné skupiny a vlastní ju organizácia predávajúca cloduové služby. Služby ponúkané týmto typom cloudu sú dostupné najširšej verejnosti. Nevýhodou je, že služba sa nedokáže prispôsobiť potrebám zákazníkov (najstarší model). Jedná sa o model, ktorý sa zameriava na uspokojovanie spoločných požiadaviek, čo najväčšej skupine potenciálnych zákazníkov. Veľkou výhodou je zas nízka cena pre užívateľov. Príkladmi verejných cloudov sú veľké spoločnosti ako Amazon Simple Storage Service (Amazon S3), Google App Engine alebo Microsoft Windows Azure. (Sosinksy, B. 2011)

Súkromný cloud

Súkromná cloudová infraštruktúra sa prevádzkuje výlučne pre potreby organizácií. Cloud môže byť riadený samotnou organizáciou alebo treťou stranou (môže byť spracovaná buď IT oddelením firmy, alebo prostredníctvom outsourcingu napr. priamo poskytovateľom riešenia na báze súkromného cloudu). Súkromný cloud sa môže nachádzať v priestoroch organizácie alebo aj mimo organizácie. Koncepcia súkromného cloudu je odpoveďou na mnohé riziká vyplávajúce z nasadenia verejného cloudu pre zákazníka. Medzi tieto riziká patrí nutnosť zdieľať cloudovú infraštruktúru s ďalšími zákazníkmi, znížená schopnosť rozhodovať o umiestnení dát a ďalšie rizika vyplávajúce z požiadaviek na dostupnosť a bezpečnosť dát. Zo známych poskytovateľov cloudu sa na oblasť súkromného cloudu špecializuje napríklad firma IBM pod názvom IBM SmartCloud Foundation.(Rouse, M. 2015)

Hybridný cloud

Hybridný cloud kombinuje niekoľko cloudov (súkromný, komunitný, verejný). Tieto cloudy zachovávajú svoju identitu, ale sú viazané dokopy ako celok. Hybridný cloud môže ponúkať štandardizovaný alebo proprietárny prístup k dátam a aplikáciám, rovnako ako prenosnosť aplikácií. Tento typ cloudu umožňuje najmä väčším firmám rozdeliť dáta a výpočtové prostriedky, s ktorými pracujú do 2 skupín: prvá skupina bude využívať služby modelu verejného cloudu, druha skupina zas bude využívať služby súkromného cloudu. Takéto triedenie môže vyplávať z rôznych obmedzení, ktoré môžu byť povahy technickej (napr. požiadavka na latenciu, šírku dátového pásma atď.), internej (napr. požiadavka ponechať definované systémy či dáta v lokalite firmy) a veľa ďalších. Hybridný cloud ponúka vyššiu flexibilitu ako samostatné modely súkromného alebo verejného cloudu, preto sa dá predpovedať, že sa v segmente veľkých korporátnych zákazníkoch stane najpoužívanejším modelom cloudových služieb. Z významných poskytovateľov cloudu sa na oblasť hybridného cloudu takisto špecializuje firma IBM pod názvom IBM SmartCloud Foundation. (Sosinksy, B. 2011)

Komunitný cloud

Komunitný cloud je založený na myšlienke zdieľať výpočtové prostriedky v rôznych organizáciách s rovnakými požiadavkami na cloudové služby, medzi ktoré patria požiadavky na miesto uloženia dát, na ich bezpečnosť a dostupnosť, požiadavky na súlad so zákonmi a pod. Koncept komunitného cloudu môže byť úspešne implementovaný pre sféru štátnej administratívy (napr. program „Federal Community Cloud For Government Organization“ ponúkaný firmou IBM štátnym inštitúciám). Nejedná sa teda o verejný cloud ani o súkromný cloud zdieľaný viacerými subjektmi.[9] Užívateľom služieb sa musia zdať zdroje cloud computingu neobmedzené. Preto je veľmi dôležité dlhodobé efektívne fungovanie prostredia a správne plánovanie výkonov a kapacít, nakoľko môže dôjsť k veľkému prebytku alebo nedostatku zdrojov.

Distribučné modely

V modeloch nasadenia boli rôzne typy cloudu vyjadrené spôsobom, akým je nasadená infraštruktúra. Ako sa cloud computing vyvíjal, rôzny predajcovia ponúkajú cloudy, ktoré majú rôzne služby. Portfólio týchto služieb pridáva ďalší súbor definícií, ktoré nazývame distribučné modely.

Poznáme rôzne distribučné modely. Všetky majú nasledujúcu formu:

XaaS, alebo „<Niečo> as a Service" („niečo" ako služba)

Tri distribučné modely boli všeobecne uznané:

IaaS (Infrastructure as a Service)

IaaS poskytuje virtuálne počítače, virtuálne úložiská, virtuálnu infraštruktúru a ostatné hardvérové prostriedky, ktoré si môžu klienti zaobstarať. Poskytovateľ služieb IaaS spravuje celú infraštruktúru, zatiaľ čo klient je zodpovedný za všetky ostatné aspekty nasadenia. Tie zahŕňajú operačný systém, aplikácie a užívateľské interakcie so systémom. (Sosinksy, B. 2011)

Príklady poskytovateľov sluzieb IaaS:

- Amazon Elastic Compute Cloud (EC2)
- Eucalyptus
- GoGrid
- FlexiScale
- Linode
- RackSpace Cloud
- Terremark

Výhody IaaS:

- Nízke počiatočné náklady
- Vlastní výber užívateľského prostredia

PaaS (Platform as a Service)

PaaS poskytuje virtuálne počítače, operačné systémy, aplikácie, služby, vývojové rámce, transakcie a riadiace štruktúry. Klient môže umiestniť svoje aplikácie na cloudovú infraštruktúru alebo používať aplikácie, ktoré boli programované pomocou jazykov a nástrojov, ktoré sú podporované poskytovateľom služby PaaS. Poskytovateľ tejto služby spravuje infraštruktúru cloudu, operačné systémy a oprávnený software. Klient je zas zodpovedný za inštaláciu a riadenie aplikácie, ktorú nasadzuje. (Sosinksy, B. 2011)

Príklady poskytovateľov sluzieb PaaS:

- Force.com
- GoGrid Cloud Center
- Google AppEngine
- Windows Azure Platform

Výhody PaaS:

- Výkon alokovaný na základe aktuálnej potreby
- Platba za priemernú spotrebu, nie za extrémy

SaaS (Software as a Service)

SaaS je kompletné operačne prostredie s aplikáciami, riadením a užívateľským rozhraním. V tomto modely je aplikácia poskytovaná klientovi prostredníctvom klientskeho rozhrania (zvyčajne prehliadač) a povinnosti zákazníka začínajú aj končia pri vkladaný a spravovaní svojich dát a riadení interakcií. Všetko ostatné od aplikácie až po infraštruktúru je zodpovednosť predajcu. (Sosinksy, B. 2011)

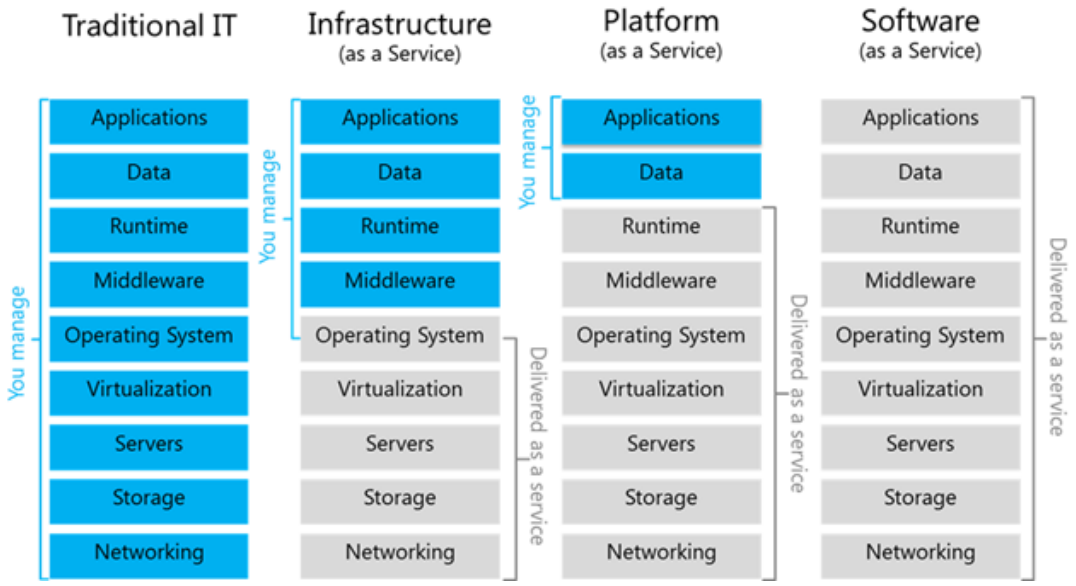
Dobré príklady poskytovateľov služieb SaaS:

- Google Apps
- Oracle on demand
- SalesForce.com
- SQL Azure

Výhody SaaS:

- Nízke počiatočné náklady
- Časté aktualizácie
- Užívateľ sa nestará o prevádzku softvéru

Obr. 3: Distribučné modely



Zdroj: https://blogs.msdn.microsoft.com/dachou/2011/03/16/rise-of-the-cloud-ecosystems/

V ostatných rokoch, keď sa do popredia dostávajú mobilné zariadenia a s nimi aj mobilné aplikácie, vznikol nový distribučný model **mBaaS (mobile backend as a service).** MBaaS je počítačová architektúra, ktorá poskytuje prístup k serverom, úložným priestorom, databázam a ostatným prostriedkom, ktoré podporujú mobilné aplikácie. Prístup MBaaS používa unifikované rozhranie pre programovanie aplikácií (API – Application Programming Interface) a nástroje pre vývoj softwaru (SDK – Software Development Kit) na prepojenie mobilných aplikácií s prostriedkami na druhej strane cloudu. MBaaS sa používa na spojenie koncových služieb a poskytuje spoločné funkcie ako posielanie upozornení, integrácia sociálnych sietí alebo polohové služby. Jedná sa o odklon od typického vývoja mobilných aplikácií, ktorý vyžaduje od vývojárov individuálne začlenenie API.(Rouse.M. 2015)

3 Analýza bezpečnosti cloud computing pre mobilné zariadenia

Cloud computing nie je obmedzený len na užívanie na osobných počítačoch. Má veľký vplyv aj na mobilné technológie. Mobilita a všadeprítomnosť sú kľúčové prvky siete budúcnosti. Teda kombinácia elektronických zariadení ako sú inteligentné smartphony, PDA, tablety, všadeprítomné mobilné siete a cloudy. Toto všetko prispelo k vzniku nového odboru: mobilný cloud computing.

Slovo „mobilita“ sa stal veľmi obľúbený pojem vo svete technológií. Došlo tiež k nárastu vo vývoji a tržieb z predaja mobilných zariadení ako sú smartphony, tablety podporujúce rôzne druhy mobilných a sieťových technológií. Ľudia si vyberajú tieto zariadenia hlavne kvôli práci a zábave.

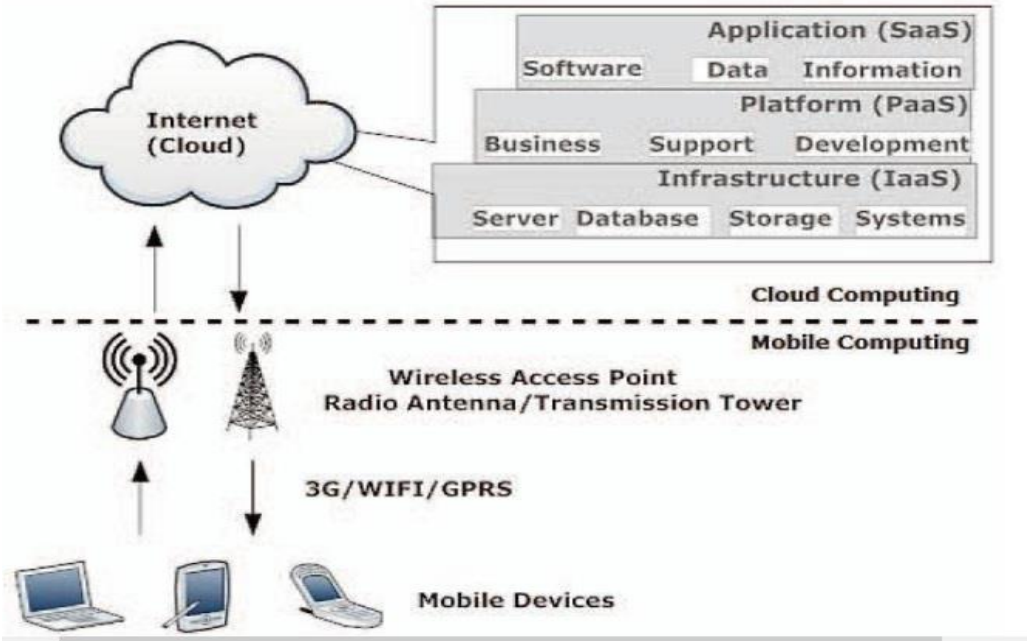
Toto nás privádza k otázke čo to vlastne mobilný computing je? Je to platforma informačného riadenia ktorá nie je závislá na mieste a čase prístupu. Autonómia tejto platformy umožňuje používateľom prístup k dátam odkiaľkoľvek a kedykoľvek. (Asrani, P. 2013) Teda či je užívateľ v pohybe alebo nie, neovplyvní to funkčnosť platformy. To, že dostupné prostriedky a výpočtová kapacita sú dostupné z akéhokoľvek miesta kde sa nachádzame, dáva tejto platforme jasnú budúcnosť.

3.1 Princípy mobilného cloud computing

Mobilný cloud computing je kombinácia mobilného computingu, cloud computingu a mobilného Internetu. Môžeme ho považovať za dostupnosť cloudových zariadení v mobilnom prostredí. Integruje výhody všetkých troch technológií a je označovaný ako cloud computing pre mobilné telefóny.

Mobile cloud computing je nový model, kde je spracovanie a ukladanie dát presunuté z mobilných zariadení do silných a centralizovaných počítačových platforiem umiestených v „oblakoch“. Na tieto platformy potom možno pristupovať pomocou bezdátového pripojenia prostredníctvom webových prehliadačov na mobilných zariadeniach. Je to podobné cloud computingu, ale strana klienta sa zmenila tak, aby to bolo uskutočniteľné na mobiloch, ale stále ide o koncept klasického cloud computingu.(Asrani, P. 2013)

Obr. 4: Distribučné modely



Zdroj: http://timesofcloud.com/cloud-tutorial/history-and-vision-of-cloud-computing

Cloud môžeme rozdeliť na mobilný computing a cloud computing. Mobilné zariadenia môžu byť smartfóny, notebooky, PDA, ktoré sú pripojené k sieti cez 3G, WIFI alebo GPRS. Používatelia mobilných zariadení môžu odosielať požiadavky na cloud aj cez webový prehliadač a prostriedky sú pridelované na základe tohto pripojenia. Po spustení webovej aplikácie sú zavedené monitorovacie a počítacie funkcie systému s cieľom zaručiť, že kvalita služby je udržiavaná až do ukončenia spojenia. To zahŕňa plnenie úloh ako rýchle posielanie odpovedí, synchronizáciu a vyrovnávanie záťaže, aby sa zabezpečilo, že prostriedky sú priďelované príslušným klientom. (Asrani, P. 2013)

3.2 Nedostatky mobilných zariadení

Hlavným cieľom mobilného cloud computingu je poskytnúť používateľom na cestách pohodlný a rýchly spôsob prístupu k údajom z cloudu pomocou svojich mobilných zariadení. Aj keď sa zvyšuje pohodlie užívateľa, stále zostáva veľa problémov v realizácii mobilného cloud computingu.

Obmedzenia mobilov

Keď sa hovorí o mobilných zariadeniach používajúce cloud computing, prvá vec, na ktorú sa treba pozerať je obmedzenie prostriedkov. Aj keď sa mobilné zariadenia zlepšili vo všetkých aspektoch (pamäť, veľkosť obrazovky, výkonnosť procesora, bezdrôtová komunikácia, operačné systémy), stále majú pri spúšťaní komplexných aplikácii vážne nedostatky ako napríklad nedostatok výpočtovej kapacity a slabá baterka. Pri porovnaní s počítačom moderné mobilné zariadenia využívajúce operačný systém iOS, Android alebo Windows Mobile znižujú schopnosť spracovania dát o 3 krát, pamäť o 5-6 krát a šírku pásma asi o 10 krát.[11] Aj keď sa tieto inteligentné telefóny dôsledne zlepšujú, stále sú tam veľké nedostatky.

Obmedzenia týkajúce sa straty siete a vybitia batérie

Ak aplikácia spotrebuje veľa batérie a potrebuje rýchle pripojenie na Internet, bude ťažké takúto aplikáciu nasadiť do mobilného zariadenia. Na prekonanie tohto problému bude musieť dôjsť k zníženiu pohybu dát a aj množstva dát prenášaných medzi mobilným zariadením a cloudovým serverovým strediskom. (Asrani, P. 2013)

Problém individualizácie mobilných zariadení

V súčasnosti existujú rôzne mobilné operačné systémy. Ak chceme vyvíjať aplikáciu pre mobilné zariadenia, musíme urobiť prostredie pre klienta čo najjednoduchšie. Jednoduché prostredie pre klienta znamená, že veľké množstvo dát môže byť uložených v cloude a funguje na každom mobilnom zariadení, bez nejakých úprav. (Asrani, P. 2013)

Kvalita služby

Rýchlosť prenosu dát v prostredí mobilného cloud computingu sa neustále mení a ak je poskytovateľ Internetu ďaleko od používateľa mobilného zariadenia, spojenie je prerušované. Oneskorenie v bezdrôtovej sieti môže byť 200 milisekúnd oproti 50 milisekúnd v káblovej sieti. Niektoré ďalšie otázky ako dynamická zmena výkonu aplikácií, mobilita používateľov, a dokonca aj počasie vedú k rozdielom v šírke pásma a siete sa prekrývajú. Z toho dôvodu je oneskorenie v mobilnej sieti vyššie ako v káblovej sieti. (Asrani, P. 2013)

3.3 Bezpečnosť a ochrana mobilného cloud computing

Zaistenie súkromia a integrity dát alebo aplikácií je jeden z kľúčových faktorov, na ktorý sa sústredia poskytovatelia služieb. Vzhľadom k tomu, že mobilný cloud computing je kombinácia mobilných sietí a cloud computingu, otázky súvisiace s bezpečnosťou sú potom rozdelené do dvoch kategórií: bezpečnosť mobilných sietí a bezpečnosť cloudu.

Bezpečnostné hrozby ako škodlivé kódy sú známe rôznym mobilným zariadeniam ako smartfóny, PDA, notebooky a podobne. Niektoré aplikácie týchto zariadení môžu spôsobiť aj problémy narušenia súkromia mobilných užívateľov.

Ochrana mobilných aplikácií – najjednoduchší spôsob ako odhaľovať bezpečnostné hrozby je inštalovanie a spúšťanie bezpečnostných softvérov a antivírusových programov na mobilných zariadeniach. Vzhľadom na to, že mobilné zariadenia majú výkonnostné obmedzenia, ich ochrana môže byť náročnejšia v porovnaní s osobnými počítačmi. Na riešenie tohto problému bolo vyvinutých niekoľko prístupov, ktoré spočívajú v prenášaní bezpečnostných mechanizmov do prostredia cloudu. Predtým, než užívatelia môžu používať určitú aplikáciu, mala by prejsť bezpečnostnou kontrolou. Všetky súbory, ktoré sú posielané do mobilných zariadení budú overené, či sú škodlivé alebo nie. (Soeung-KonN, K. – Jung-Hoon, L. – Sung- Woo, K. 2012)

Ochrana súkromia – poskytovanie osobných údajov a našej aktuálnej polohe môže ohroziť naše súkromie. Napríklad použitie Location Based Services (LBS) poskytované GPS zariadeniami môže ľahko odhaliť našu polohu. (Soeung-KonN, K. – Jung-Hoon, L. – Sung-Woo, K. 2012).

4 Analýza bezpečnostných prvkov troch poskytovateľov

V následujúcej časti je zhrnutá analýza bezpečnostných prvkov troch poskytovateľov.

	Amazon Web Services	**Google Cloud Platform**	**Microsoft Azure**
Fyzické zabezpečenie	profesionálny personál, kamerový systém, systém detekcie prieniku, MFA, požiarny systém, záložný generátor, pravidelná kontrola, preventívna údržba, chladiaci systém	profesionálny personál, prístupové karty, alarmy, biometria, detektory kovov, laserové lúče, kamerový systém, pravidelná kontrola, ochranka, požiarny systém, záložný generátor, chladiaci systém	bezpečnostný personál, alarmy, kamerový systém, prístupové karty, biometria, požiarny systém, záložný generátor, chladiaci systém, ochrana proti zemetraseniu
Počet dátových centier	12	15	22
IAM	AWS IAM	Google IAM	Azure Active Directory
SAML	áno	áno	áno
OAuth	OAuth 2.0	OAuth 2.0	OAuth2.0
MFA	áno	áno	áno
Šifrovanie	áno	áno	áno
SSL/TLS	áno	áno	áno

Cerifikácia			
PCI DSS1	áno	áno	áno
HIPAA	áno	áno	áno
SSAE16 SOC1	áno	áno	áno
SSAE16 SOC2	áno	áno	áno
SSAE16 SOC3	áno	áno	áno
ISO27001	áno	áno	áno
ISO27017	áno	áno (od 15.4.2016)	nie
	Amazon Web Services	**Google Cloud Platform**	**Microsoft Azure**
ISO27018	áno	áno (od 15.4.2016)	áno
CSA	áno	nie	áno
FedRAMP	áno	áno	áno
FISMA	áno	áno	áno
Zabezpečenie siete			
Shared Cloud Network	áno	nie	nie
VPN	áno (VPC)	áno (subnet)	áno (Vnet)
VPN medzi dátovými centrami	nie	áno	nie
Firewall	áno	áno	áno
Bezpečnostné rozšírenia pomocou protokolu IPSec	áno	áno	áno
Vzdialený prístup na cloudový server	SSH	SSH	SSH
Prevádzková bezpečnosť			
Ochrana proti Malwaru a DDoS útokom	áno	áno	áno
Monitorovanie a zaznamenávanie	áno	áno	áno
Podpora	nonstop	nonstop	nonstop

Ako je vidieť z tabuľky bezpečnosť je pre týchto porovnávaných poskytovateľov veľmi dôležitá. Komplexné zabezpečenie služieb od fyzického zabezpečenia cez sieťové až softvérové je na veľmi vysokej úrovni. Jednotlivé bezpečnostné prvky týchto poskytovateľov sú veľmi podobné a líšia sa len minimálne, čo upevňuje ich postavenie. Firmy ako Amazon, IBM, Google a Microsoft sú podstatnými lídrami svetové trhu a prebieha medzi nimi silná konkurencia. To znamená, že tieto firmy sa stále predbiehajú a dobiehajú a stále prichádzajú s niečím novým, a tým sa snažia získať zákazníka na svoju stranu. Vzhľadom k tomu že priemysel IKT je v dnešnej dobe veľmi dynamický, práve aktuálnosť, inovatívnosť a maximálna bezpečnosť sú veľmi dôležité atribúty z pohľadu zákazníka.

5 Záver

Úpech mobilného cloud computing napreduje veľmi rýchlo. Ale stále sú tu nedostatky, ktoré treba riešiť a stále posúvať túto technológiu na vyššiu úroveň s vedomím, že cloud computing používa veľká časť pracovne aktívnej populácie. Analýzou týchto nedostatkov sme zistili, čo prinesie budúcnosť v oblasti mobilného cloud computingu. Vedci navrhujú optimálny a efektívny spôsob prideľovanie šírky pásma, obmedzená šírka pásma stále predstavuje obrovskú obavu, pretože počet mobilných a cloudových užívateľov sa radikálne zvyšuje. Preto by sa mali ďalšie štúdie snažiť začleniť technológie ako 4G alebo dokonca 5G aby prekonali tento problém.

V budúcnosti sa môže vyskytnúť situácia, keď jeden „mrak“už nebude stačiť potrebám používateľov mobilných zariadení. Z toho dôvody je potrebný nový model, aby používatelia mohli využívať služby z viac cloudov jednotným spôsobom. Jedným z možných riešení je napríklad „Sky Computing“, ktorý je ešte o úroveň vyššie ako cloud computing. Sky computing jednoducho znamená využitie prostriedkov z viacerých cloudov a vytvoriť tak distribuovanú štruktúru. Podobne aj mobilný cloud computing umožní svojim užívateľom podporiť túto „medzioblakovú komunikáciu“a takisto nasadzovať ďalšie mobilné aplikácie a služby. Na naplnenie všetkých týchto požiadaviek stačí sa zaoberať otázkou, ako dosiahnuť konvergenciu služieb.

Literatúra

[1] Antonopoulos, N., & Gillam, L. (2010). *Cloud computing: priciples, systems and applications* (ISBN 978-1-84996-240-7). London, Springer.

[2] Asrani, P. (2013). Mobile Cloud Computing. Retrieved May 09, 2017, from http://www.ijeat.org/attachments/File/v2i4

[3] Chellappa, R. (2012). Emory University: Goizueta Business School. Retrieved April 09, 2017, from http://www.bus.emory.edu/ram/

[4] Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. Retrieved April 30, 2016, from http://nvlpubs.nist.gov/nistpubs/Legacy/SP

[5] Naumann, F. (2009). *Dějiny informatiky: od abaku k internetu* (ISBN 978-80-200-1730-7). Praha: Academia.

[6] Parkhill, D. F. (1966). *The Challenge of the computer utility* Addison-Wesley Publishing Company ed., (ISBN 978-20177-00593). Reading, GB: Mass., London.

[7] Pugh, E. W., Johnson, L. R., & Palmer, J. H. (1991). *IBM's 360 and early 370 systems* (ISBN 0-262-16123-0). Cambridge, MA: MIT Press.

[8] Rouse, M. (2015). Mobile Backend as a Service (mobile BaaS). Retrieved from http://searchmobilecomputing.techtarget.com/definition/mobile-Backend-as-a-Service-mobile-BaaS.

[9] Soeung-Kon, K., Jung-Hoon, L., & Sung- Woo, K. (2012). Mobile Cloud Computing Security Considerations. Retrieved January, 2016, from http://www.sersc.org/journals/JSE/

[10] Sosinsky, B. (2011). *Cloud computing bible* (ISBN 978-0-470-90356-8). Chichester, Indianapolis: John Wiley & Sons.