Mendelova univerzita v Brně
Provozně ekonomická fakulta

Implementace cloud computingu v podnikovém a univerzitním prostředí – utajení, integrita a dostupnost dat

Disertační práce

Vedoucí práce:
doc. Ing. Ivana Rábová, Ph.D.

RNDr. Zuzana Priščáková

Brno 2015

Rada by som poďakovala svojej školiteľke doc. Ing. Ivane Rábovej, Ph.D. za vedenie tejto práce.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Implementace cloud computingu v podnikovém a univerzitním prostředí – utajení, integrita a dostupnost dat** vypracovala samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*
Jsem si vědoma, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.
Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brne, dňa 28. mája 2015 .....

Abstract

Prišč áková, Z. Cloud computing in corporate and university environments - security, availability and data integrity. Dissertation thesis. Brno, 2015.

The goal of the dissertation thesis is the methodical contribution to area of security of the data stored using cloud computing. The theses deal with the current problem of the data security in virtualized environment. The emphasis is on security from the perspective of cryptography, availability and integrity of the data. For general use of the proposed methodic, the verification of the methodic is performed in an enterprise and university environment. In the first chapter, there's an overview of the present literature about the cloud computing, storing the data, data security, and the integrity of the data. These terms are further specified using descriptions of each algorithms, protocols, norms, and rules. In this part, there's also pointed the problem of the security in the enterprise and university environment. In the second chapter, the results of the dissertation thesis are presented. The own solutions are divided into individual parts according to the chronology of the research. In the introductory subchapter, there's a proposal of solution this data security issue analyzed from the detailed view on the life-cycle of the stored data and the actors of the proposed system. The proposal of the model includes definitions of the security modules, the view on the model from the perspective of actors and the realization, the determination of security rules of the proposed model, and identification of the data life-cycle. In the mentioned parts, there's an outline of the final steps and the definition of the methodic. The formalization of the proposed methodic is converted using the determination of the security aspects, determination and verification of the methodic with use of the finite non-deterministic machine and Petri nets. The particular results are summarized into the final methodic of the increase of the security of data stored into cloud, from the perspective of the implementation of the cloud computing in the enterprise and university environment. The proposed methodic is generalized using the determination of the basic steps, proposal of the architecture and the infrastructure of the cloud computing. Verification of the methodic is further more characterized via the description of the implementation and testing. The last subchapter of the results of the research shows the opportunity of the solution of data availability issue. The proposal of the solution is mathematically derived and tested in the simulation environment. The result of this case study is summarized in the final assessment. In the discussion and the conclusion, there are summarized the main outputs of the research, and the new opportunities of solution – the security

of data from the perspective of classification of the data in cloud computing, and the classification of the cloud computing itself – are outlined, too.

Abstrakt

Prišťáková, Z. Implementace cloud computingu v podnikovém a univerzitním prostředí - bezpečnost, dostupnost a integrita dat. Dizertačná práca. Brno, 2015.

Cieľom dizertačnej práce je metodický prínos v oblasti zabezpečenia dát ukladaných do cloud computingu. Práca sa zaoberá aktuálnym problém z oblasti bezpečnosti dát vo virtualizovanom prostredí. Dôraz je kladený na bezpečnosť z pohľadu kryptografie, dostupnosti a integrity dát. Pre všeobecné využitie navrhnutej metodiky je verifikácia metodiky prevedená v podnikovom a univerzitnom prostredí. Obsah prvej kapitoly sa zameriava na prehľad súčasnej literatúry zameranej na cloud computing, ukladanie dát, bezpečnosť dát a integritu dát. Uvedené termíny sú bližšie špecifikované prostredníctvom popisov jednotlivých algoritmov, protokolov, noriem a pravidiel. V tejto časti je taktiež poukázany problém riešenia bezpečnosti v podnikovom a univerzitnom prostredí. V druhej kapitole sú prezentované výsledky dizertačnej práce. Vlastné riešenia sú rozdelené do jednotlivých častí s ohľadom na chronologickosť výskumu. V úvodnej podkapitole je predstavený návrh riešenia bezpečnosti dát ukladaných do cloud computingu z detailnejšieho pohľadu na životný cyklus ukladaných dát a aktérov navrhnutého systému. Návrh modelu zahrňuje definovanie bezpečnostných modulov, pohľad na navrhnutý model z hľadiska aktérov a realizácie, stanovenie bezpečnostných pravidiel navrhnutého modelu a identifikovanie životného cyklu dát. V uvedených častiach sú naznačené výsledné kroky a definície metodiky. Formalizácia navrhnutej metodiky je prevedená determinovaním bezpečnostných aspektov, stanovením a overením metodiky pomocou využitia konečného nedeterministického automatu a Petriho siete. Jednotlivé výsledky sú zhrnuté do finálnej metodiky zvýšenia zabezpečenia dát ukladaných do cloudu z pohľadu implementácie cloud computingu v podnikovom a univerzitnom prostredí. Navhnutá metodika je generalizovaná determinovaním základných krokov, návrhu architektúry a infraštruktúry cloud computingu. Verifikácia metodiky je detailnejšie charakterizovaná popisom implementácie a testovania. Záverečná podkapitola výsledkov výskumu poukazuje na spôsob riešenia dostupnosti dát. Návrh riešenia je matematicky odvodený a testovaný v simulačnom prostredí. Záver tejto prípadovej štúdie je zhrnutý vo výslednom zhodnotení. V diskusii a závere sú zhrnuté hlavné výstupy výskumu a načrtnuté nové možnosti riešenia bezpečnosti dát z pohľadu klasifikácie dát v cloud computingu a klasifikovania cloud computingu.

Obsah

Zoznam obrázkov

1 Úvod a cieľ práce

1.1 Úvod do problematiky

Vývoj výpočtovej a telekomunikačnej techniky sa za posledné desaťročia posúva radikálnymi skokmi. Pri práci denne využívame nové výdobytky výpočtovej techniky, či už v podobe stolných počítačov, notebookov, smartfónov, tabletov a podobne. Pre zvýšenie možností komunikácie a urýchlenie práce, pracujeme prostredníctvom Internetu z rôznych miest Zeme, kde dosahuje pokrytie celosvetovej siete Internetu. Dostupnosť Internetu sa neustále zvyšuje a môžeme povedať, že už pomaly ani neexistuje podnik vo vyspelých krajinách, ktorý by pre svoje fungovanie nepotreboval niektorý z uvedených výdobytkov modernej doby. Prostredníctvom výpočtovej techniky umožňujeme stálu dostupnosť dát potrebných pre chod firmy v akomkoľvek čase z akéhokoľvek miesta. (Prišťáková, 2013)

Taktiež ako napreduje vývoj hardvéru, postupuje aj vývoj softvéru, ktorý je čoraz náročnejší na výpočtové prostriedky a úložiská dát. Aby firmy udržali krok s dobou a nárokmi nových aplikácií, musia častejšie aktualizovať svoj hardvér. Tieto aktualizácie si vyžadujú periodicky značnú časť finančných prostriedkov a aj personál, ktorí sa o aktualizáciu musí postarať. Nie len stabilné firmy, ale aj každá novovznikajúca firma potrebuje výpočtovú techniku a softvér s licenciami, ktorých zakúpenie pri novovznikajúcej firme je vysoko nákladné. (Prišťáková a Rábová, 2013)

Najdrahším, ale najjednoduchšie realizovateľným riešením je ukladanie dát v lokálnej sieti (LAN). Výhodou LAN je vysoký výkon a dostupnosť ukladania dát cez ustálené rozhrania firiem. Životnosť serverov, nutnosť zálohovania a obnovy systému, kúpa licencií, ukázali, že toto riešenie nebolo tým najsprávnejším. Azda za zanedbateľnú nevýhodu sa považuje fyzické umiestnenie siete. LAN je energeticky závislá, a tak vplýva aj na environmentálne problémy Zeme. Z tohto dôvodu bolo potrebné riešenie odkloniť od fyzickej vrstvy.

K dnešným trendom v oblasti informačných technológií radíme cloud computing. Pod pojmom cloud computing si môžeme predstaviť mrak plný dát (Rouse, 2012). Každý deň využívame technológiu cloudu bez toho, aby sme vnímali, že naše dáta nie sú uložené na konkrétnom mieste, ale v abstrakcii. Cieľom tejto technológie je poskytovanie služieb, aplikácií uložených na serveroch poskytovateľa cloudového riešenia. (Prišťáková, 2013)

Hlavnou podmienkou prístupu k dátam, je prístup na Internet. Prístup k dátam je umožnený v akúkoľvek hodinu a z akéhokoľvek miesta. Prístup môže byť umožnený aj cez webový prehliadač. Cloud computing je biznis model s disponovaním diskovej kapacity, vysokého výkonu a výpočtovej kapacity serverov s použitím virtualizácie. Gartner definoval cloud computing ako štýl computingu, v ktorom sú informačné technológie škálovateľné a pružné s podporou dodávania ako služby pomocou internetových technológií (Gartner, 2012).

Cloud computing predstavuje novú flexibilnú paradigmu poskytovania IT služieb. Cloud ako výkonné hostingové riešenie reprezentuje model pay-as-you-go, ktorý

umožňuje spoločnostiam škálovať ich infraštruktúru tak, aby zodpovedala rastu spoločnosti (Rybár, 2012). Teda výhoda použitia cloudu pre firmy spočíva v princípe platenia iba za to, čo firma použije. V prípade nedostačujúcej kapacity, poskytovateľ služby umožní plynulé rozšírenie bez zmien vyvolaných na doposiaľ uložených dátach.

Cloud computing je nazývaný aj green cloud, nakoľko poskytuje lacné a prakticky neobmedzené úložisko údajov. Prezývku green cloud získal aj vďaka nižším energetickým potrebám a environmentálnej záťaži. Vzhľadom na zvolený cloudový model, ponúka programovanie vlastných aplikácií v cloudovom prostredí podniku. K jeho veľkým výhodám taktiež zaraďujem automatickú aktualizáciu, čím sa odbúra zdĺhavé postupné preinštalovanie verzií aplikácií. Táto výhoda má avšak aj negatívum, ktoré spočíva v zamedzení prístupu k starým verziám aplikácie, či operačného systému, a teda používateľ je nútený pracovať vždy s aktuálnou verziou.

K negatívam technológie cloud computingu radím problémy s ukladaním dát, bezpečnosťou, prístupom k dátam. Výrazným deficitom je rýchlosť, ktorá klesla z dôvodu využívania obmedzených pásiem. Ukladanie dát do cloudu je založené na sieťovom pripojení medzi LAN a poskytovateľom úložiska údajov v cloude (Kallahalla, Riedel, Swaminathan, Wang a Fu, 2003). Jeho vysoká citlivosť na sieť (pri výpadku siete) môže spôsobiť úplnú nedostupnosť. Častým problémom s cloudom je aj konsolidácia s firmou (Sullivan, 2012).

Bezpečnosť v cloude vychádza z jeho vlastnosti - viacnásobnosť. Cez sieť sa dokážeme pripojiť na príslušný server, kde sa nachádza používateľská aplikácia. Vďaka aplikácii sa dostávame k dátam. Pri práci s dátami sú dôležité bezpečnostné podmienky. K bezpečnostným podmienkam radím integritu dát, ich utajenie a dostupnosť. Tieto bezpečnostné podmienky sa aplikujú na citlivé dáta. Týmto termínom označujem všetky údaje, ktoré nie sú určené verejnosti, údaje, ktoré spadajú pod zákon ochrany osobných údajov, obchodné tajomstvo, heslá a podobne.

SEC (securities and exchange commision) (Virginia´s community colleges, 2012) definoval citlivé dáta ako všetky údaje, ktoré kompromisne s rešpektovaním dôvernosti, integrity a/alebo dostupnosti, majú výrazný negatívny vplyv na správanie agentúrnych programov, alebo súkromie, na ktoré jednotlivci majú nárok. Citlivé údaje sú priamo úmerné závažnosti kompromisu údajov s ohľadom na tieto kritériá. Agentúry musia klasifikovať každý IT systém príslušnou citlivosťou podľa množstva citlivých údajov, ktoré IT systém ukladá, spracováva, alebo prenáša (Sebe, Domingo-Ferrer, Martinez-Balleste, Deswarte a Quisquater, 2008). Pri integrite sa využívajú autentizačné kódy, ktoré sa priradia po zašifrovaní dát (Boneh a Franklin, 2001). K šifrovaniu dát pomocou kľúčov sa využívajú princípy kryptografie.

Poslednou podmienkou je dostupnosť. Týmto termínom označujem fyzické riešenie pripojenia servera na energetický zdroj. Aktuálnym riešením je závislosť na elektrickom prúde. Pri výpadku prúdu môže dôjsť k úplnej alebo čiastočnej strate dát, zamedzeniu prístupu k dátam a aplikácii uloženej v cloude.

Zo súčasných možností sa javí zavedenie cloud computingu do podnikového a univerzitného prostredia ako riešenie problému s úložiskom dát, s prácou s dátami

a napokon aj zníženie nákladov oproti súčasnému riešeniu.

1.2 Cieľ a metodika práce

Cieľom dizertačnej práce je metodický prínos v oblasti zabezpečenia ukladaných dát s využitím technológie cloud computingu v podnikovom a univerzitnom prostredí. Zadaný cieľ práce bude dosiahnutý porovnaním správania sa cloudu pri ukladaní dát, pričom budem prihliadať na odlišné prostredia implementovanej technológie. Bezpečnosť dát uložených v cloude bude prezentovaná na základe troch faktorov – utajenie dát, integrita dát a dostupnosť. Dôraz je kladený na bezpečnosť dát z hľadiska integrity dát.

Výsledkom práce bude návrh modelu a rámcovej metodiky pre zvýšenie bezpečnosti a integrity dát ukladaných do cloudu. Navrhovaná metodika bude vychádzať z protokolov, noriem a doposiaľ známych algoritmov pre zabezpečenie a ukladanie dát do virtualizovaného prostredia. Metodika bude verifikovaná v prostredí univerzity a strednej firmy. Výsledky verifikácie budú zovšeobecnené.

Ku splneniu cieľa práce budú naplnené tieto kroky:

- vymedzenie základných pojmov, definícií, metodík, noriem, protokolov a algoritmov v kontexte bezpečnosti dát ukladaných do cloudu,
- analýza cloudového modelu SaaS ako úložiska dát,
- identifikovanie etáp životného cyklu virtuálneho stroja,
- analýza súčasných riešení bezpečnostných podmienok utajenie, dostupnosť a integrita dát,
- analýza podnikového a univerzitného prostredia z hľadiska nasadenia cloud computingu,
- zostavenie modelu zvýšenia bezpečnosti dát ukladaných do cloudu na základe aktuálne dostupných noriem, protokol, algoritmov ako aj komunikácie s malými a strednými podnikmi a univerzitami využívajúcimi cloud,
- simulácia a analýza simulácie navrhovaného modelu,
- formalizácia modelu a jeho vyjadrenie pomocou metodiky,
- implementácia modelu a metodiky v podnikovom a univerzitnom prostredí,
- analýza výsledkov testovania,
- diskusia zameraná na implementáciu modelu a metodiky pre malé a stredné podniky, a univerzity.

Vytýčený cieľ a kroky docielim pomocou využitia aktuálne dostupnej zahraničnej literatúry z oblasti zabezpečenia cloud computingu, využitím platených a open-source technológií a softvérov (KVM, ZFS, Enterprise Architect, HPSim, MATLAB,

Voltcraft), konzultáciami s expertami v danej oblasti a účasti na vedeckých a odborných konferenciách (zbieranie nových poznatkov).

1.3 Štruktúra práce

Daná práca je rozdelená z hľadiska obsahu na dve časti. Prvú časť tvorí literárna rešerš zameraná na virtualizáciu, cloud computing, ukladanie dát v cloude a bezpečnosť ukladaných dát. Tieto teoretické východiská predstavujú komplexný súhr informácií z 74 zdrojov zahraničnej literatúry a 17 zdrojov tuzemskej literatúry.

V úvodnej podkapitole popisujem základné termíny z oblasti cloud computingu ako sú virtualizačný architekt, hypervízor, životný cyklus virtuálneho stroja a 5 základných faktorov cloud computingu. Obsahom druhej podkapitoly je predstavenie problému, ktorý bližšie popisujem a riešim vo vlastnej práci. Táto časť je zameraná na predstavenie základného princípu ukladania dát v cloud computingu, komplexného riešenia pre redundanciu dát a ich zabezpečenie. V tretej podkapitole charakterizujem detailnejší pohľad na bezpečnosť dát v cloude, pričom poukazujem na možnosti zmiernenia rizík.

Obsahom štvrtej podkapitoly je detailný pohľad na integritu dát v cloude. Integrita dát je primárnym problémom, ktorý riešim vo vlastnej práci. Táto podkapitola je tvorená úvodnou časťou, kde špecifikujem typy poškodenia dát a nosnou časťou, v ktorej komplexne zhrňuje doposiaľ známe riešenia integrity dát na základe protokolov a algoritmov. V závere tejtočasti uvádzam verifikáciu integrity dát a popisujem využitie cloud computingu v podnikovom a univerzitnom prostredí, pričom poukazujem na rozdiely. Zhrnutie teoretických východísk uvádzam v zhrnutí podkapitoly, kde špecifikujem stanovené problémy vyplývajúce z uvedenej literárnej rešerše.

Druhá kapitola dizertačnej práce sumarizuje nadobudnuté výsledky. Túto kapitolu delím na štyri časti z pohľadu riešenia stanoveného problému a dosiahnutia cieľa predkladanej práce. V prvej podkapitole definujem navrhnutý model zvýšenia bezpečnosti dát uložených v cloud computingu. Tento model popisujem z pohľadu bezpečnostných modulov, aktérov systému a realizácie, stanovenia bezpečnostných pravidiel a identifikovania životného cyklu dát. Obsah tejto časti naznačuje pricíp navrhnutej metodiky. Druhá časť podkapitoly je zameraná na stanovenie metodiky, pričom využívam formalizáciu konečného deterministického automatu a Petriho siete. V tretej podkapitole opisujem výsledky testovania formalizovanej metodiky v podnikovom a univerzitnom prostredí. Záverečná časť obsahuje zhrnutie výsledkov a ich využitie v praxi.

Súhrn dôležitých informácií druhej kapitoly je naznačený v diskusii. Cieľom diskusie je poukázanie na vnímanie zvoleného problému dizertačnej práce z pohľadu všeobecného, a neskôr aj z pohľadu styku s verejnosťou (konferencie, stáž, ohlasy od čitateľov).

Významnou časťou práce je príloha, v ktorej sa nachádzajú podporné grafické materiály k výsledkom práce. V Prílohe A je znázornený podľad na navrhnutý model pomcou využitia diagramu prípadov použitia. Príloha B obsahuje bližší popis na

navrhnutý model pridaním rozšírených väzieb. Obsahom Prílohy C je kontingenčná tabuľka vzájomných väzieb medzi prípadmi použitia, modulmi a aktérmi. Príloha D reprezentuje statický pohľad na navrhnutý model prostredníctvom diagramu tried. Obsah Prílohy E je zameraný na znázornenie zabezpečenia ukladaných dát v cloude prostredníctvom sekvenčného diagramu. Prílohy F, G a H špecifikujú štrukturované aktivity uvedené v hlavnom diagrame aktivít. V Prílohe I je znázornená vytvorená Petriho sieť. Obsahom prílohy J je konečný nedeterministický automat.

2 Teoretické východiská práce

V dizertačnej práci sa opieram o tri bezpečnostné podmienky (utajenie, integrita a dostupnosť), na základe uvedených podmienok od Winklera (Winkler, 2011), Mathera (Mather, Kumaraswamy a Latif, 2009) a Rhotona (Rhoton a Haukioja, 2013).

Mather (Mather, Kumaraswamy a Latif, 2009) poukazuje na zaujímavý problém so *šifrovaním dát* ukladaných do cloudu. Popisuje dva odlišné prístupy k utajeniu dát, a to buď dáta najprv zašifrovať, a až potom uložiť do cloud, alebo dáta uložiť do cloudu nešifrované, a až tak použiť šifrovací mechanizmus pri opätovnom načítaní. Bližšie daný problém nepopisuje. Za výhodnejšie šifrovacie mechanizmy považuje šifry založené na symetrickom šifrovaní. Symetrické šifry oproti asymetrickým šifrám majú iba jeden šifrovací kľúč.

Mather (Mather, Kumaraswamy a Latif, 2009) za najvhodnejšie šifry zvolil Triple DES (dĺžka kľúča je 112 bitov) a AES (dĺžka kľúča je 128 bitov). Tu je dôležité poznamenať, že Winkler (Winkler, 2011) uvádza ako vhodný šifrovací systém RSA, ktorý má byť použitý pred uložením dát do cloudu. Hoff (Hoff, Mogull a Balding, 2013) uvádza použitie hashovacieho algoritmu SHA-256, ktorý by priebežne utajoval dáta. Lim (Lim, Coolidge a Hourani, 2013) sa taktiež prikláňa ku šifrovaciemu systému RSA. Práve tu sa ponúkajú otvorené otázky kedy je vhodné dáta zašifrovať a aký algoritmus je najvhodnejší pre utajenie dát. V rámci dizertačnej práce chcem odpovedať na tieto otázky.

Pre riešenie *integrity dát* Hoff (Hoff, Mogull a Balding, 2013) uvádza kontrolu prostredníctvom API (application programming interface), teda rozhranie pre programovanie aplikácií. Mather (Mather, Kumaraswamy a Latif, 2009) popisuje riešenie integrity dát prostredníctvom priradenia authentizačných kódov (MACs). Mather (Mather, Kumaraswamy a Latif, 2009) uvádza, že na šifrovanie dát je vhodné použiť blokový symetrický algoritmus v móde reťazení blokových šifier CBC (cipher block chaining) a zahrnúť jednosmernú hashovaciu funkciu. Winkler (Winkler, 2011) popisuje, že je dôležité si uvedomiť, či potrebujeme integritu udržiavať vo veľkej firme, alebo v malom podniku. Jeho myšlienku chcem ďalej rozvinúť v dizertačnej práci a poukázať na vhodný spôsob dodržania integrity dát v cloude.

Dostupnosť dát bližšie špecifikuje najmä Mather (Mather, Kumaraswamy a Latif, 2009), ktorý opisuje najznámejšie prípady s problémom dostupnosti, ich následky ako aj udanie dostupnosti v rámci prepojenia času, dňa, mesiaca, roku a percentuálneho vyjadrenia dostupnosti. Taktiež poukazuje na dôležitosť dokumentu o poskytovaní služieb – SLA (service-level agreement) (Popa, Lorch, Molnar, Wang a Zhuang, 2011). Lim (Lim, Coolidge a Hourani, 2013) poukazuje na problém dostupnosti vyplývajúci z dokumentu SLA. Návrh riešenia dostupnosti dát v cloude je jedným z bodov zamerania výskumu dizertačnej práce.

2.1 Virtualizácia a cloud computing

Základom cloud computingu bolo objavenie *virtualizácie*. S virtualizovaním v informačných technológiách sa stretávame v rôznych úrovniach. Hlavnú zmenu spôsobilo virtualizovanie operačného systému hostu, prípadne servera (Priščáková a Rábová, 2012).

Cieľom virtualizácie serverov je súbežný beh viacerých izolovaných operačných systémov s použitím jedného hardvéru (Rouse, 2012). Z cieľu virtualizácie voľne vyplýva jej definícia – softvér, ktorý vytvára virtuálne prostredie medzi serverom a operačným systémom. Dittner a Rule (Dittner a Rule, 2007) zadefinovali virtualizáciu ako rámec alebo metodiku rozdelenia zdrojov počítačového hardvéru do viac exekučných prostredí, použitím jedného alebo viacerých pojmov alebo technológie, ako sú hardvérové a softvérové časti, časové zdieľanie, čiastočná alebo úplná simulácia stroja, emulácia a kvalita služieb.

Virtualizácia

Základy virtualizácie sú podľa Ruestových (Ruest a Ruest, 2010) tvorené tromi úlohami:

- virtualizačný architekt – preskúmaním všetkých vrstiev virtualizácie dostávame vzájomné prepojenie jednotlivých vrstiev s dátovým centrom. Algoritmus prieskumu prebieha nastieňovaním častí postupu tvoreného piatimi krokmi (spoločnosť Resolutions to ponúka pre implementáciu virtuálnej infraštruktúry už niekoľko rokov),
- vytvorenie virtualizačnej infraštruktúry – jej cieľom je po vytvorení previesť všetky podrobné kroky, ktoré je potrebné použiť pre prevedenie dátového centra na dynamické dátové centrum. Výhodou dynamického dátového centra je dynamické reagovanie na všetky obchodné potreby,
- konsolidácia výhod – v tejto časti sa ukončuje prechod k virtualizácii pohľadom na to, ako sa zmenia návyky dátového centra so zavedením virtuálnej infraštruktúry.

Pri virtualizácii sa zachováva konzistencia medzi virtualizovaným a nevirtualizovaným prostredím. Komunikácia medzi týmito prostrediami prebieha prostredníctvom štandardnej sieťovej komunikácie. Virtualizovať môžeme aj operačný systém hosta, čo sa označuje termínom softvérová vrstva, ktorá umožňuje odhaliť fyzické prostriedky a sprístupniť ju niekoľkým rôznym virtuálnym počítačom súčasne (Dittner a Rule, 2007). Počítač umožňuje bežne beh iba jednej inštancie operačného systému, a teda ak chceme súčasne pracovať pod dvomi operačnými systémami, potrebujeme mať dva fyzické stroje. Použitím virtualizácie rozdelíme jeden fyzický počítač na niekoľko virtuálnych strojov, pričom každý z nich používa svoj vlastný virtuálny hardvér a obsahuje vlastné inštancie operačného systému, ktoré sú od seba izolované (Ahson a Ilvas, 2011).

Technológia virtualizácie operačného systému hostu existuje v týchto variantách (Ruest a Ruest, 2010):

- softvérová vrstva sa využíva pre simuláciu fyzického počítača nad operačným systémom bežiacim aktuálne na hardvérovom hoste,
- softvérový engine, teda hypervízor, niekedy nazývaný aj ako virtual machine monitor, beží priamo nad hardvérom a eliminuje réžie sekundárneho operačného systému.

Cieľom *hypervízora* je riadiť a spravovať jednotlivé virtuálne jednotky – stroje. Pod spravovaním chápem aj sprostredkovanie prístupu k virtuálnym procesorom, pamäti, diskom, sieti a podobne. Tým, že sa vytvorí virtuálny hardvér na hoste, je potrebné zamedziť prístup virtualizovaných jednotiek ku reálnym fyzickým jednotkám hardvéru (procesor, pamäť, atď.) a súčasne aj k virtuálnym strojom navzájom. Vzhľadom na umiestnenie hypervízora, môžem povedať, že existujú dva typy (Dittner a Rule, 2007):

- typ 1 beží priamo na fyzickom hardvéry,
- typ 2 je nainštalovaný na hosťujúcom operačnom systémom, nad ktorým potom bežia jednotlivé virtuálne stroje, teda guesty.

Medzi typom 1 a typom 2 existuje hybrid. Hybridný typ beží taktiež na fyzickom hardvéri ako typ 1, ale je závislý na systémovej podpore a driveroch zariadenia virtuálneho stroja. Takýto virtuálny stroj sa nazýva privilegovaná doména. Pod týmto termínom chápem virtuálny stroj, ktorý má zvláštne práva pre riadenie hypervízora a ďalších domén.

Virtuálny stroj bežiaci nad hypervízorom je označovaný ako doména. Ich počet je prakticky neobmedzený, nakoľko jediné obmedzenie je výkon hardvéru. Operačné systémy, ktoré bežia v doménach sa nazývajú geusty. Každá doména, okrem privilegovanej domény, nemá právo na riadenie ďalších domén, a taktiež jej nie je umožnený prístup k fyzickému hardvéru, ktorý je pridelený druhým doménam.

Životný cyklus virtuálneho stroja

Tak ako fyzické počítače, aj virtuálne stroje majú svoj životný cyklus. V dynamickom dátovom centre sú fyzické počítače používané výlučne ako hostovské servery. Z toho vyplýva, že ich životný cyklus je pomerne krátky. *Životný cyklus* je tvorený zo štyroch fáz, ktoré nie sú výrazne odlišné od fáz životného cyklu fyzických počítačov.

Životný cyklus je znázornený na obrázku 1 a je zložený z týchto fáz(Ruest a Ruest, 2010):

- *plánovanie (modrá farba)* – v tejto fáze je dôležité určiť správny výber nasadenia. Po výbere prebieha príprava riešenia nasadenia,

Obr. 1: Životný cyklus virtuálneho počítača (Ruest a Ruest, 2010)

- *príprava a nasadenie (zelená farba)* – jej cieľom je získať a vytvoriť balíčky, nastaviť konfiguráciu, následne previesť inštaláciu a otestovať nasadenie. Ide o najdlhšiu a najnáročnejšiu fázu životného cyklu,
- *prevádzka (žltá farba)* – úlohou prevádzky je spravovanie problémov, správy o zmenách, optimalizovanie ako aj správy o prevádzkovej sieti. Táto fáza si vyžaduje rovnakú časovú záťaž ako plánovanie,
- *vyradenie (červená farba)* – slúži pre správne naplánovanie doby určenej pre nahradenie, prípadne upgradovanie, odstránenie zastaraných technológií a procesov. Táto fáza je najkratšou a najjednoduchšou oproti doposiaľ uvedeným fázam životného cyklu.

Cloud computing

V úvode bola stanovená definícia *cloud computingu* podľa spoločnosti Gartner. Podrobnejšia charakteristika cloud computingu vyplýva z definície podľa inštitútu NIST (National Institute of Standards and Technology) (Mell a Grance, 2011). V tejto charakteristike vystupujú 4 modely použitia, respektíve nasadenia – verejný, súkromný, hybridný a komunitný cloud (Rouse, 2012). Inštitút NIST neberie do úvahy vládny cloud, keďže ide o veľmi špecifické riešenie cloud computingu určené iba pre vládne orgány.

Mell a Grance (Mell a Grance, 2009) využili charakteristiku cloudu inštitútom NIST, a tak spresnili základné charakteristiky cloud computingu a rozdelili ich na 5 faktorov:

- samoobslužné služby v prípade potreby (on demand self-service) – samoobslužné služby sú orientované na používateľa cloudu, ich hlavnou výhodou je možnosť zabezpečenia servera a úložiska dát používateľom, z tohto vyplýva odprostenie od poskytovateľa cloudu,
- široký prístup k sieti (broad network access) – výhodou širokého prístupu k sieti je pokrytie všetkých požadovaných funkcií v rámci siete používateľa, pokrytie funkcií je zabezpečené využitím tenkého a hrubého klienta,
- združovanie zdrojov (resource pooling) – podstatou združovania zdrojov je spájanie dostupných zdrojov poskytovateľa cloudu za účelom dosiahnutia modelu multinájmu, model multinájmu umožňuje využívanie zdrojov viacerým používateľom cloudu, v rámci tohto modelu sú zdroje rozdelené poskytovateľom cloudu na základe požiadaviek používateľov cloudu,
- rapídna pružnosť (rapid elasticity) – rapídna pružnosť cloud computingu vyplýva z možností zmien kapacity cloudu, veľkosť kapacity narastá rapídne a jej pružnosť je prispôsobená na základe požiadaviek používateľa cloudu, na základe tohto faktu platí všeobecné tvrdenie, že z pohľadu používateľa je kapacita neobmedzená ani vzhľadom na veľkosť, ani vzhľadom na čas,

- merateľná služba (measured service) – merateľná služba v cloud computingu je zameraná na kapacitu v rámci zvolenej úrovne abstrakcie, merateľná služba je spúšťaná automaticky a jej cieľom je kontrola a optimalizácia aktuálne dostupných zdrojov používateľa, na základe výsledkov kontroly je možné vytvoriť správu o využívaní zvolených služieb určenú pre používateľa ale aj poskytovateľa cloudu.

2.2 Ukladanie, ochrana a bezpečnosť dát v cloud computingu

Nakoľko výskum dizertačnej práce sa zameriava na bezpečnosť dát v cloude, považujem za vhodné prebádať ukladanie dát v cloude, na ktoré priamo nadväzuje integrita dát obsiahnutých v cloude.

Ukladanie dát v cloude

Ukladanie dát v cloude môžeme považovať za pomerne atraktívnu formu outsourcingu zameraného na každodennú správu dát (Sosinsky, 2011). Napriek tomuto tvrdeniu, ale reálna zodpovednosť za správu údajov spadá pod spoločnosť, ktorá vlastní dáta. S ohľadom na túto skutočnosť, je dôležité pochopiť niektoré z príčin poškodenia dát. K takýmto príčinám patrí udržanie veľkej zodpovednosti poskytovateľa cloudových služieb, niektoré základné osvedčené postupy pre využitie bezpečného ukladania dát do cloudu, ako aj metódy a normy pre sledovanie integrity dát bez ohľadu na uloženie dát (Winkler, 2011). Pre docielenie vyššej bezpečnosti a dodržania redundancie dát sú dáta ukladané súčasne v cloude aj lokálne (Hurwitz, 2013).

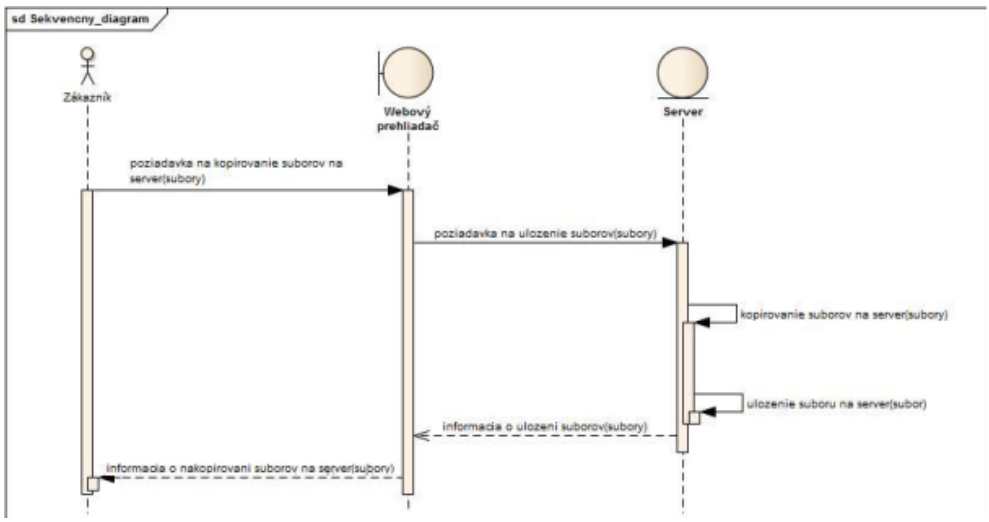
Jednou z hlavných výhod ukladania dát do cloudu, je neobmedzený prístup k dátam, pričom neobmedzenosť spočíva v čase a mieste prístupu. Túto vlastnosť využijú firmy, ktorých pracovná činnosť prebieha v rôzne vzdialených lokalitách. Pre takéto firmy sa oplatí vstúpiť do cloudového riešenia aj z dôvodu minimalizovania záťaže na fyzické úložné zariadenia, používanie rovnakého počítača a viacnásobný prístup k dátam v reálnom čase (real-time reporting) (Winkler, 2011).

V tomto prípade je dôležité pri vytváraní úložiska cloudu myslieť aj na špecializáciu úložiska. Aj keď existuje niekoľko stoviek úložísk cloudu, každé úložisko je orientované na iné požiadavky, napríklad ukladanie komunikácie prostredníctvom e-mailu, ukladanie profilov zamestnancov, ukladanie dokumentácie projektov a podobne (Winkler, 2011). Pravdaže požiadavkou môže byť aj ukladanie všetkých typov dokumentov.

Komunikácia dátového serveru a klienta

S rastúcim počtom dát sa zvyšuje aj počet požadovaných serverov. Pre základný funkčný beh cloudového úložiska je potrebný jeden dátový server pripojený do siete Internet.

Komunikácia medzi dátovým serverom a klientom (zákazník poskytovateľa cloudu) prebieha na základe požiadavky pre uloženie do cloudu (Nielsen, 2013).



Obr. 2: Sekvenčný diagram interakcie ukladania dát medzi klientom a dátový serverom

Táto komunikácia je zobrazená na obrázku 2 prostredníctvom UML sekvenčného diagramu. Rozhraním pre komunikáciu je webový prehliadač. Parametrom pre túto komunikáciu sú súbory, ktoré boli zvolené pre uloženie na server.

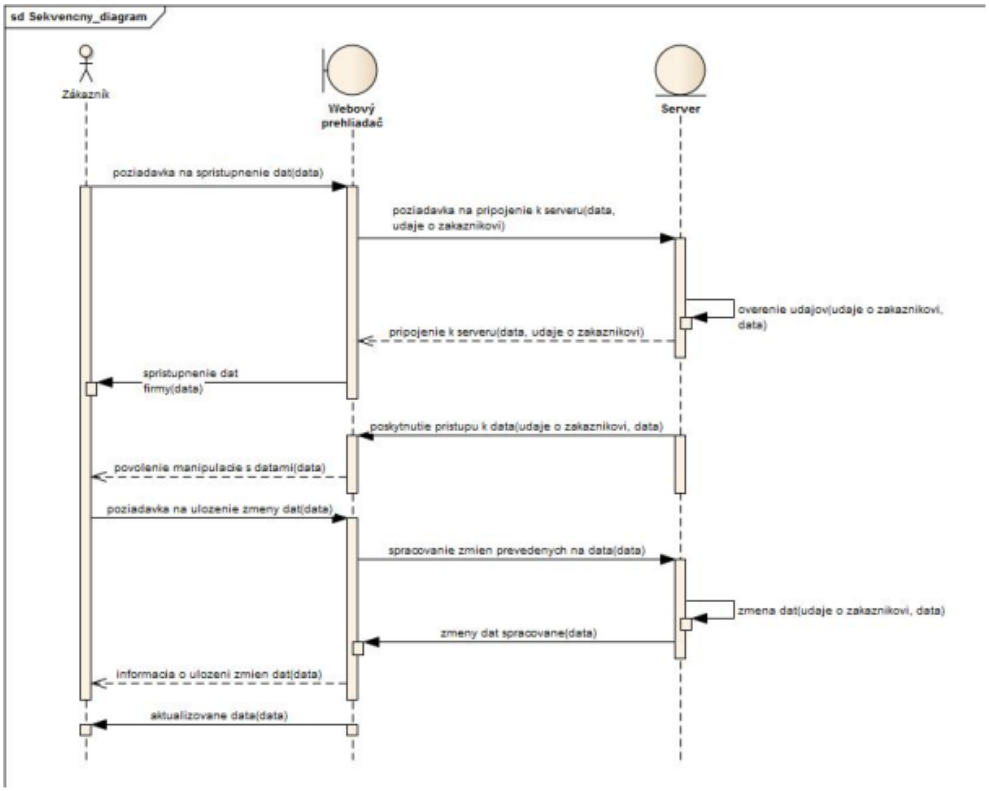
V prípade požadovania prístupu k dátam zo strany klienta, komunikácia medzi klientom a serverom by prebiehala podľa sekvencie znázornenej na obrázku 3 (Erl, Puttini a Mahmood, 2013).

Pravdaže dátový server vždy posiela, alebo sprístupňuje iba dáta, ktoré patria klientovi, respektíve dáta, ku ktorým má prístup v prostredí firmy. Modelovú situáciu ukladania a prístupu k dátam v cloude uvádzam pre ukážku základného princípu, avšak je dôležité poznamenať, že v skutočnosti úložiská cloudu využívajú stovky dátových serverov, pričom sa zahrňujú aj servery pre udržanie redundancie. Je to z toho dôvodu, že servery je potrebné udržovať, opravovať, a teda je potrebné dáta uložiť do viacerých miest.

Redundancia dát

Redundanciou v sieti LAN (local area network) sa rozumie doplnenie jedného (prípadne dvoch) záložných serverov v dátovom centre pre prípad problému (Lim, Coolidge a Hourani, 2013). Nakoľko aktuálne sa využívajú možnosti virtualizácie, tak redundancia predstavuje naklonovanie virtuálneho serveru na rovnakom zariadení, prípadne naklonovanie všetkých virtuálnych serverov jedného zariadenia na druhý fyzický server, a tak dosiahnutie vytvorenia tieňových kópií.

Eswaran a Abburu (Eswaran a Abburu, 2012) uvádzajú jednoduchý algoritmus ukladania dát do cloudu. Pre vstupnú inicializáciu algoritmus využíva údaje o súbore, vlastníkovi dát, cloudovom servery, tajnom a šifrovacom kľúči. Hlavná



Obr. 3: Sekvenčný diagram interakcie prístupu a zmeny dát medzi klientom a dátovým serverom

myšlienka algoritmu znázorňuje, že na cloudový server sú ukladané iba tie súbory, ktoré sú zjednotené so šifrovacím kľúčom.

Eswaranov algoritmus ukladania dát do cloudu

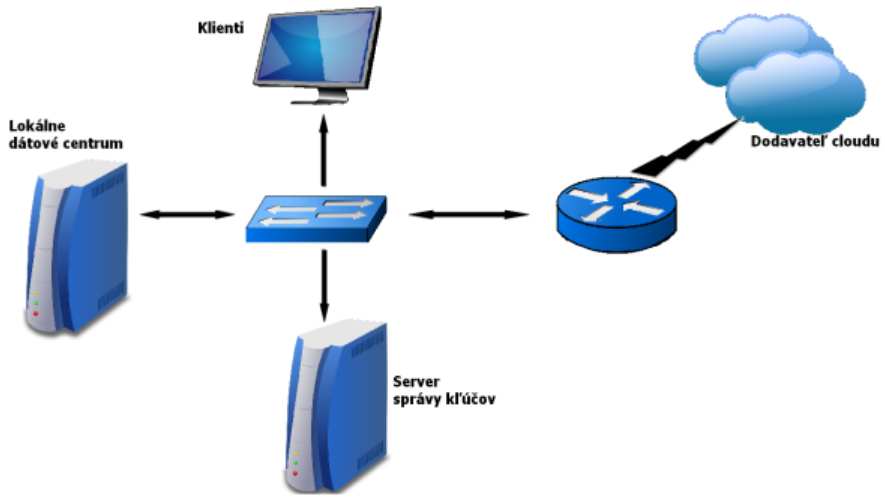
```
F :=subor;
Cc:=dataVlastnika;
Cs:=cloudovyServer;
Tkluc:=tajnyKluc;
Skluc:=sifrovaciKluc;
begin
if (hodnota=Tkluc) then prihlasenie:=true
else begin
showMessage(Neopravneny pristup);
prihlasenie:=false;
end;
Cs:=F (F $\cup$  Skluc);
end;
```

Keby cloud nespĺňal podmienku redundancie, popieral by aj jeho základnú charakteristiku, a teda prístup klienta do cloudu k uloženým dátam v akýkoľvek čas. Keďže väčšina systémov ukladá rovnaké dáta na servery s rôznymi zdrojmi napájania, tak môžu klienti bez problémov pristupovať ku svojim dátam pri zachovaní redundancie. Z toho vyplýva, že používanie cloudu ako úložisko dát firmy nie je jednoduché, a teda nejde o priame hostovanie firemného servera v dátovom centre poskytovateľa cloudového riešenia (Wang, Wang, Li, Ren a Lou, 2009), ale dáta sú rozdelené na niekoľko častí (Mather, Kumaraswamy a Latif, 2009), pričom jednotlivé časti môžu byť rozptýlene aj v rámci celej Zemi.

Keďže poskytovateľ cloudu spravuje redundantný systém, dáta sa opäť roztrúsia v rámci celého cloudu. Poskytovateľ z týchto dôvodov nezaisťuje redundantné služby priamym pripojením ďalšieho serveru, ale zmenou prideľovania prostriedkov s cieľom dosiahnuť redundantný systém (Lim, Coolidge a Hourani, 2013). Je vhodné upozorniť, že pri zachovaní uvedených podmienok poskytuje cloud aj úroveň zabezpečenia dát pred odcudzením (Erl, Puttini a Mahmood, 2013), nakoľko chyba v lokálnej sieti by mohla znamenať trvalú stratu, zatiaľ čo v cloude o svoje dáta firmy neprídu.

Zabezpečenie dát

Pre *zabezpečenie* dát v cloude používa väčšina systémov kombináciu jednotlivých metód pre zabezpečenie dát. Najrozšírenejšia metóda je *šifrovanie*. Pomocou šifrovacích systémov dostávame zakódované dáta. K ich dekódovaniu je potrebný šifrovací kľúč, a preto aj keď je možné dostať sa k týmto zašifrovaným dátam, problém je dostať sa ku ich kľúču k rozšifrovaniu.



Obr. 4: Diagram správy kľúčov v cloude

Obrázok 4 znázorňuje diagram siete správy kľúčov, ktoré využíva kryptografia. Dôležitým prvkom diagramu je server, ktorý má za úlohu *správu kľúčov*. Server uchováva transportné, autentizačné a odvolávacie kľúče (Winkler, 2011). Taktiež má na starosti správu autorizačných tokenov, certifikátov, ako aj kľúčov určených pre šifrovanie súborov a kľúčov hardvérového úložiska.

K jednoduchším metódam pre zabezpečenie dát patrí bežne používaná *autentifikácia klienta*. Autentifikačný systém (proces) povolí prístup k dátam na základe správne zadaného mena a hesla (Mather, Kumaraswamy a Latif, 2009). Táto metóda patrí k jednoduchším aj z dôvodu jej zvýšenej možnosti prelomenia (Erl, Puttini a Mahmood, 2013). Okrem autentifikačných procesov poznáme aj autorizačné postupy, ktoré taktiež poskytujú prístup používateľa k dátam, avšak v tomto prípade klient poskytne zoznam osôb, ktoré majú oprávnenie pristupovať k dátam uloženým v cloude (Rhoton a Haukioja, 2013).

Keďže firma má viacero druhov dát, je potrebné vytvoriť rovnaký počet *úrovní identifikácie*. Teda aký je počet skupín dostupnosti dát, taký je aj počet úrovní. Dostupnosťou dát v tomto prípade myslím právomoci jednotlivých zamestnancov firmy, keďže iné práva má bežný zamestnanec a iné práva má generálny riaditeľ firmy. S autorizačnými postupmi sa stretávame bežne vo firemnom prostredí.

Aj keď šifrovanie a autentizácia predstavujú bezpečnostný systém, ktorým môžeme zabezpečiť svoje dáta u poskytovateľa cloudu, vždy tu zostáva otvorená otázka bezpečnosti dát vzhľadom k vzdialenému úložisku dát. Kedykoľvek sa dostanú dáta mimo vlastné dátové centrum firmy, môže nastať ich odcudzenie. Je dôležté si uvedomiť, že poskytovateľ cloudového úložiska má viacero klientov, a teda dáta svojej firmy môžu byť uložené hneď pri dátach konkurenčnej firmy. Z tohto faktu vyplýva reálna hrozba odcudzenia dát práve konkurenciou.

Možnosťou ako zabezpečiť túto situáciu na strane klienta je práve šifrovanie a *zabezpečenie prenosu dát technológiami typu SSL* (secure socet layer) (Mather,

Kumaraswamy a Latif, 2009). Je potrebné si uvedomiť, že k odcudzeniu dát môže prísť aj zo strany nespokojného zamestnanca, a preto je vždy potrebné uvažovať nad povolením jednotlivých autorizačných úrovní. Príkladom odcudzenia dát zamestnancom je jednoduchá situácia, kedy odosielam svoje citlivé dáta do cloudu prostredníctvom protokolu SSL, a tak plne dôverujem svojim programátorom. Súbory môže ohroziť aj drobná chyba v podobe vynechania písmena s pri prenose dát *protokolom HTTPS* (hypertext transfer protocol secure) (Rhoton, Clercg a Graves, 2013). A taktiež netreba zabúdať na nastavenie latencie (Lim, Coolidge a Hourani, 2013). So zvyšujúcou sa latenciou hrozí aj vyššie riziko odcudzenia.

Úložisko ako služba

S ukladaním dát do cloudu je vhodné uviesť aj druhotný význam akronymu SaaS, a teda *Storage as a Service* (úložisko ako služba) (Marsh, 2011). V tomto prípade ide o poskytnutie služby úložiska dát poskytovateľa cloudu koncovým používateľom, ktorí nechcú mať vlastné úložisko (nechcú si ho zriadiť) (Wang, Wang, Li, Ren a Lou, 2009). K tejto možnosti pristupujú väčšinou malé a stredné podniky, ktoré buď nemajú vlastné oddelenie informačných technológií, prípadne majú málo skúseností so správou infraštruktúry.

Hlavnou výhodou takýchto typov úložísk je zníženie nákladov. Úložisko si firma prenajme na základe platby za uložený gigabajt, alebo prenesené dáta. Koncoví používatelia teda nemusia platiť za infraštruktúru, ale iba za to, koľko dát prenesú a uložia na serveroch poskytovateľa. Pokiaľ požiadavky na kapacitu dát sú nepostačujúce na strane poskytovateľa, poskytovateľ túto situáciu vyrieši veľmi jednoducho, a to pridaním ďalších štandardných pevných diskov (Ayad a Dippel, 2011).

Pri termíne Storage as a Service je potrebné uviesť, že klient opäť pracuje prostredníctvom softvéru, kde si vyberie dáta pre zálohovanie, a až potom ich prenesie po spojoch WAN (Marsh, 2011). Ak by došlo k strate dát, klient si môže kedykoľvek svoje dáta stiahnuť od poskytovateľa. Poniektorí poskytovatelia využívajú aj archivovanie dát, a to kopírovaním na disky DVD. V prípade straty dát a požiadavky vydania dát zo strany zákazníka, mu poskytovateľ dodá iba daný disk obsahujúci kopírované dáta.

Zhrnutie podkapitoly

Výhodou cloud computingu ako úložiska dát je neobmedzený prístup k dátam. Ukladanie dát prebieha na základe komunikácie medzi klientom (koncovým pou žívateľom) a dátovým serverom. Klient komunikuje prostredníctvom rozhrania webu zadávaním požiadaviek pre prácu s dátami. Server vyhodnotí tieto po žiadavky a vykoná potrebné inštrukcie. Ukladanie dát prebieha na základe redundancie, čím sa dosiahne určitý stupeň zvýšenia bezpečnosti. K najjednoduchším metódam zabezpečenia patrí autentifikácia používateľa (prihlásenie na základe mena a hesla). Pre vyššiu bezpečnosť dát je vhodnejšie využívať šifrovanie dát a priradenie autentizačného kódu pre dáta. Pre šifrovanie a zabezpečenie prenosu na strane klienta sa

využijú technológie typu SSL. Z doposiaľ uvedených teoretických východísk nie je presne stanovená architektúra cloud computingu z pohľadu bezpečnosti, preto bol v rámci formalizácie metodiky smerovaný výskum aj na inicializovanie jednotlivých blokov architektúry, pričom boli testované uvedené možnosti a zvolené najvhodnejšie riešenie.

2.3 Bezpečnosť dát

Bezpečnosť dát možno definovať ako zachovanie dôvernosti a integrity údajov spracúvaných organizáciou (Erl, Puttini a Mahmood, 2013). V tejto podkapitole sa zameriam na tieto dve časti, ktoré sú základom pre výskum popísaný v dizertačnej práci.

Zmiernenie rizík zabezpečenia dát

V scenároch, kde vlastník údajov nemá detailnú kontrolu nad architektúrou a ovládacími prvkami riadenia, napríklad outsourcing, predpokladám zvýšené riziko zabezpečenia dát. Zmierniť riziká môžem pomocou poznania nasledujúcich prvkov (Mather, Kumaraswamy a Latif, 2009), (Erl, Puttini a Mahmood, 2013), (Rhoton, Clercg a Graves, 2013):

- *organizačná štruktúra*, ktorá náležite cení, chráni a používa dáta, a to ako pri plánovaní, tak aj pri poskytovaní služieb,
- *silné a jasné postupy zodpovednosti*, ktoré uznávajú, že vlastník údajov (organizačná jednotka) je najlepším miestom na pochopenie a riešenie rizík pre ich informácie, vrátane osobných údajov,
- *opatrenia* vykonávané pre úroveň zabezpečenia archivovaných dát, vytvorenie dôvernosti, zabezpečenia dát a ich zdieľania,
- *stanovenie jasnej politiky*, ktorá má byť jednoduchá na pochopenie a použitie,
- *ovládanie externých častí podniku*, pochopenie, čo dodávatelia firmy robia a ich kontrola podľa potreby,
- *poskytnutie* konzistentného a univerzálneho rámcu školenia bezpečnosti,
- *ujasnenie si životného cyklu dát* spojených so zamestnancami firmy.

Schéma klasifikácie dát

V rámci bezpečnosti dát sa často v podnikovom prostredí využíva *schéma klasifikácie dát* (Rhoton, Clercg a Graves, 2013). Jej cieľom je bližšie poukázať na potrebné ovládacie prvky jednotlivých dátových typov, ktoré sú spracovávané podnikom. Schéma

klasifikácie dát sa vypracuje na základe právnych, regulačných a obchodných požiadaviek, ktoré firma musí dodržiavať (Winkler, 2011). V bežnom podnikovom prostredí sa využívajú tri režimy (prípadne 4):

- *verejné/nezaradené* (napr. marketingové materiály),
- *vnútorné použitie* (informácie zdieľané v rámci organizácie alebo s dodávateľmi, napríklad intranet),
- *dôverné/súkromné* (citlivé informácie, napríklad údaje o kreditnej karte),
- *tajné* (trhovo citlivé informácie, napríklad výsledky ku koncu roka).

Všeobecné zásady ochrany osobných údajov

Pri bezpečnosti dát je dôležité uviesť fakt, že neexistujú všeobecné zásady, ktorými by sa mohla firma riadiť pri zabezpečení ochrany dát. Existujú avšak *normy pre zásady ochrany osobných údajov* (Poynter, 2008). Poynter (Poynter, 2008) stanovil desať základných pravidiel pre zabezpečenie ochrany dát, o ktorých môžem povedať, že majú všeobecnejší charakter:

- *údaje o entite* (jedná sa o jednotlivca alebo podnik) sú prisúdené danému objektu a predstavujú základné všeobecné informácie o entite. Tieto údaje sú dostupné aj iným stranám, pričom ale vlastníkom údajov je iba majiteľ subjektu,
- *povinnosťou subjektu* je udržiavať svoje údaje,
- *údaje sa stávajú informáciami*, keď majú pre podnik významnú hodnotu. Zvyčajne k tomu dochádza prostredníctvom agregácie a kontextu. Vytýčeným cieľom v tomto prípade je dosiahnutie minimálnej až nulovej straty informácií a znemožnenie nechcených prístupov k informáciám. Aby sa tento cieľ dosiahol, využíva sa segregácia. Segregáciou sa oddelia dáta pri ukladaní a určia sa pracovné miesta a systémy, ktoré informácie vyžadujú,
- firma by mala mať *minimálne údaje* požadované na *výkon svojich funkcií*, vrátane uchovávania pre udržanie dát. Nemali by sa udržiavať dáta, ktoré je možné získať z iného zdroju, ale v prípade bežných dát by sa mal využiť externý zdrojov údajov (nie spojený s firmou), čím sa docieli zlepšenie schopnosti prispôsobiť svoje služby svojim zákazníkom,
- podnik by mal *udržiavať všetky údaje o danej entite spolu* a nerozdeľovať ich do viacerých úložísk. Vhodnou štruktúrou ukladania dát by bolo presunutie údajov o entite do jedného záznamu zákazníka pre jednotlivcov a jeden záznam o zákazníkovi pre podnik,
- *pre efektívne zabezpečenie informácií* je dôležité, aby zákazník aj poskytovateľ služieb zohrával svoju rolu. Firmy by mali mať právomoci, aby mohli apliko-

vať bezpečné metódy výmeny údajov so svojimi zákazníkmi, počnúc podnikom a časom vrátane jednotlivcov,

- *podniky by mali prihliadať na externé zdroje* usmernení o bezpečnosti informácií, ako napríklad právne predpisy o ochrane údajov a pokynov pre sektor finančných služieb,
- *bezpečnostné opatrenia dát* by mali byť zamerané na oblasti najväčšieho rizika akým je prenos dát. Prevody digitálnych dát týkajúcich sa fyzického média by mali byť čo najmenšie,
- *komunikácia prebiehajúca prostredníctvom tlačenej verzii* (papierové dokumenty) by sa mala zracionalizovať po obsahovej a frekvenčnej stránke s dlhodobým plánom ich výraznej eliminácie,
- *počítače* (a v krátkom čase iné vymeniteľné médiá) by mali byť *zašifrované* tak, aby zamedzili prístup k akýmkoľvek údajom alebo informáciám.

Zhrnutie podkapitoly

Z uvedenej bezpečnostnej charakteristiky môžem vyvodiť záver – pre udržiavanie dát je vhodnejšie mať vo firme zabezpečenú oblasť podniku, ako je dátové centrum a dáta neukladať do prenosných počítačov, prípadne na iné zariadeniach, ktoré sa nachádzajú vo verejných priestoroch. Technológia tenkého klienta, ako je prehliadač alebo terminálové relácie, umožňujú prístup k aplikáciám (Hugos a Hulitzky, 2011), ale pre ukladanie dát v dátovom centre je potrebná konfigurácia, ktorá zabráni lokálnej tlači a ukladaniu na iné médium.

Ak dáta je nutné uložiť na prenosné zariadenia alebo počítače, ktoré prichádzajú do kontaktu s verejnými priestormi, je potrebné dáta šifrovať. Identifikačné, autentizačné a autorizačné ovládacie prvky sú kľúčové pre riadenie prístupu k informáciám o základných vlastnostiach dát. Pre neštruktúrované dátové typy, ako sú e-maily, tabuľky a dokumenty textového procesora, je vhodné použiť nástroj DLP (data loss prevention), kde budú mať pravdepodobne vyššiu hodnotu prevencie (Hanningan, 2008). DLP nástroje môžu zistiť aké dátové typy sú prenášané a ukladané do informačného systému podniku, a taktiež určenie obchodných pravidiel s týmito údajmi, pričom je možné údaje uložiť, vytlačiť alebo odoslať.

Z tejto podkapitoly vyplynula nízka identifikácia a nejednotnosť medzi stanovenými postupmi pri zabezpečení dát ukladaných do cloudu. Vzhľadom k uvedeným riešenia bol zostavený model zvýšenia bezpečnosti dát ukladaných do cloudu, pričom model vychádzal z uvedených postupov zmiernenia rizík, klasifikácie dát a všeobecných zásad ochrany údajov.

2.4 Integrita dát

Všetky dáta firmy a využívajúce softvéry v cloudovej technológii sú uložené na serveroch na vzdialenom mieste – *dátové centrá*. Prostredie dátového centra umožňuje podnikom spúšťať aplikácie rýchlejšie so zjednodušenou správou a menším úsilím na údržbu, a oveľa rýchlejšie škálovať zdroje (servery, úložisko, sieť) vzhľadom k potrebám (Wang, Wang, Li, Ren a Lou, 2009). Dátové centrum v cloudovom prostredí obsahuje informácie, ktoré sú väčšinou uložené na počítačoch koncových používateľov (Kuyoro, Ibikunle a Awodele, 2011).

Podľa Chena a Zhaa (Chen a Zhao, 2012) takýto typ dátového centra vzbudzuje veľké obavy vzhľadom k ochrane používateľského súkromia. Pohyb dát v centralizovaných službách by mohol mať vplyv na súkromie a bezpečnosť interakcie koncových používateľov so súbormi uloženými v pamäťovom priestore cloudu. Podľa Ninga (Ning, Cong, Ming, Kui a Wenjing, 2014) použitie virtualizovanej infraštruktúry ako odrazového mostíku môže zaviesť nové útoky na *integritu dát* používateľa. Dáta pri integrite sú definované ako presné a konzistentne uložené dáta pri absencii akýchkoľvek modifikácií dát medzi dvoma aktualizáciami súboru alebo záznamu (Zeng, 2008). Cloudové služby by mali zabezpečiť integritu dát a zaistiť dôveru v používateľskom súkromí (Leka, 2013).

Aj keď outsourcing dát v cloude je ekonomicky atraktívny vzhľadom k nákladom a zložitosti dlhodobého rozsiahleho ukladania dát (Singh a Liu, 2008), stále chýba ponuka silnej záruky integrity dát a možnej dostupnosti nezávislosti v rámci širokého pokrytia podnikov a jednotlivých používateľov cloudu (Sun, 2014). Cloud computing predstavuje v prvom rade obavu z hľadiska *ochrany osobných údajov*, pretože poskytovateľ služieb v každom okamihu môže pristupovať k dátam, ktoré sú uložené v cloude (Williams, 2010). Poskytovateľ cloudu môže náhodne alebo zámerne zmeniť alebo odstrániť niektoré informácie z cloudových serverov (Zeng, 2008). Preto systém musí mať nejaký mechanizmus, ktorý zabezpečí integritu dát.

Integrita dát predstavuje relevantnosť dát, ich konzistenciu ako aj dostupnosť (Rhoton, Clercg a Graves, 2013). Pri ukladaní dát do cloudu koncový používateľ predpokladá, že dáta (prípadne aplikácie, s ktorými pracuje vo virtualizovanom prostredí) sú patrične zabezpečené. Akýkoľvek bezpečnostný cloudový model je založený na predpoklade, že používateľ (zákazník) by mal veriť vo svojho poskytovateľa cloudu. Táto dôvera sa spisuje dokumentom SLA, ktorý všeobecne vymedzuje vzájomné očakávania a povinnosti poskytovateľa a koncového používateľa (Popa, Lorch, Molnar, Wang a Zhuang, 2011).

Monitorovanie integrity dát v cloude je potrebné pre ukladanie dát v cloude. Výsledkom monitorovania môže byť aj poškodenie dát.

Poškodenie dát

Poškodenie dát môže dôjsť v ktorejkoľvek úrovni skladovania. Bit rot (oslabenie alebo strata bitov dát na médiách úložiska), regulátor poruchy, deduplikácie metadát

poškodenia, páskové poruchy, to všetko radím k príkladom rôznych typov médií spôsobujúcich poškodenie (Marsh, 2011).

Metadáta poškodenia môžu byť výsledkom niektorého z vyššie uvedených chýb, ale tie sú citlivé na softvérové chyby mimo sadzieb hardvérových chýb (Marsh, 2011). Avšak, vedľajším účinkom je to, že deduplikácie poškodeného súboru, bloku, alebo bitu ovplyvňuje všetky súvisiace časti dát viazaných na tieto metadáta. Pravdou je, že k poškodeniu dát môže dôjsť kdekoľvek v prostredí úložísk. Dáta môžu byť poškodené jednoduchou migráciou na inú platformu, teda aj odosielaním dát do cloudu (Erl, Puttini a Mahmood, 2013).

Úložiská dát cloudu sú dátové centrá s hardwarom a softwarom, ktoré sú neustále vystavené možnému poškodeniu údajov. Takýmto príkladom je zlyhanie Amazonu v roku 2011, kedy došlo ku strate dát zákazníkov (strata bola o veľkosti 0,07 percent). Amazon vtedy vyhlásil, že strata bola spôsobená obnovením premenlivých dátových snímkov z ... (Erl, Puttini a Mahmood, 2013). Hlavná podstata teda bola v poškodení dát v systéme Amazon a ako výsledok sa prejavila v strate zákazníckych dát.

Protokol o dohode jednotlivých úrovní služieb

Je dôležité rozumieť právnej zodpovednosti cloudových služieb na strane poskytovateľa aj zákazníka. Medzi týmito stranami sa uzatvára *protokol o dohode jednotlivých úrovní služieb* (SLA). Cieľom tohto protokolu je špecifikovať zabezpečenie ochrany dát v každom kroku manipulácie s dátami firmy (Winkler, 2011). Rovnako ako u mnohých právnych dokumentov, sú SLA často písané v prospech poskytovateľa, nie pre zákazníka (Popa, Lorch, Molnar, Wang a Zhuang, 2011).

Mnoho poskytovateľov cloudových služieb ponúkajú rôzne vrstvy ochrany. Napriek tomu v SLA je poskytovateľ cloudu v tomto dokumente často pozbavený zodpovednosti za integritu dát (Popa, Lorch, Molnar, Wang a Zhuang, 2011). SLA jazyk obsahuje explicitné príkazy chrániace cloudového poskytovateľa v prípade, ak sú dáta stratené alebo poškodené (Marsh, 2011).

Predpokladom ochrany údajov k distribúcii rizika je, že sa minimalizuje pravdepodobnosť straty dát. Aj keď ukladanie dát v cloude požaduje, aby primárna kópia a záloha dát boli uložené spoločne, prístup k dátam nie je závislý na výkone siete alebo pripojenia (Rhoton, Clercg a Graves, 2013). Pri dodržaní týchto základných osvedčených postupov a poznaní detailov SLA dokumentu poskytovateľa cloudu, je vhodné zaviesť metódu pre proaktívne sledovanie integrity dát bez ohľadu na platformu úložiska alebo umiestnenia (Marsh, 2011).

Protokol o vyňatí

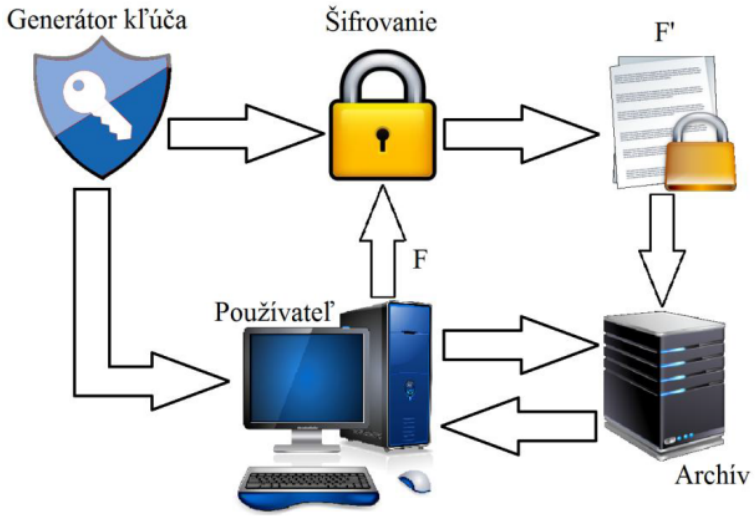
Pri zmene dát, prípadne ich vymazaní môže dôjsť k zlyhaniu, a preto je potrebné overiť, či dáta boli skutočne odstránené, alebo ich zmena bola zaznamenaná. Väčšinou pre overenie zmeny si používateľ dané dáta stiahne z cloudu. Pri veľkom objeme

dát ide o zdĺhavú činnosť. Stanovenie integrity dát môže byť prohibitívne prostredníctvom podmienok zvýšených nákladov na šírku pásma a času, najmä v prípade, ak sú potrebné časté kontroly údajov (Eswaran a Abburu, 2012).

Protokol (doklad) o vyňatí (POR – proof of retrievability), respektíve dôkaz o opätovnom vybratí, znamená overenie dát uložených koncovým používateľom na vzdialenom úložisku v cloude, bez zmeny cloudu (Juels a Kaliski, 2007). Tento protokol je povinný zabezpečiť, že dáta sú načítané iba overeným majiteľom. POR sa nazýva aj strážcami, v prípade veľkých súborov (Neha a Murthy, 2012).

Protokol založený na vkladaní náhodného strážcu v dátovom súbore

Sravan a Saxena (Sravan a Saxena, 2012) navrhli základnú schému protokolu na základe *vkladania náhodného strážcu v dátovom súbore*. Táto schéma je znázornená na obrázku 5. Súbor v schéme je označený písmenom F (file). Podstata schémy spočíva v predpoklade, že koncový používateľ cloudu chce uložiť súbor do cloudu (na server). Pred uložením súboru do cloudu je potrebné súbor zašifrovať. Zašifrovaním sa dosiahne zabránenie pred neoprávneným prístupom.



Obr. 5: Schéma protokolu na základe vkladania strážcu (Sravan a Saxena, 2012)

Schéma sa zaoberá rôznymi aspektmi, ktoré sú považované za dosiahnutie integrity. Spoločnosť, ktorá má ako úložisko dát zvolený cloud, má byť oprávnený používateľ a je registrovaná ako klient. Pre každého oprávneného používateľa systém vygeneruje bezpečnostný kľúč. Tajný kľúč je použitý pre vlastníka, ktorý sa potrebuje prihlásiť. Majiteľ môže získať tajný kľúč buď v režime off-line, alebo on-line. Ak je vlastník on-line, tajný kľúč je zaslaný do jeho pošty.

Navrhovaný systém zaisťuje, že neoprávnení používatelia nemajú povolenie prihlásiť sa. Oprávnený používateľ môže klientovi nahrať súbor do cloudu. V čase nahrávania súborov do cloudu navrhovaného systému je kľúčový prvok generátor, ktorý

generuje kryptografické kľúče a odošle ich majiteľovi. Pri každom súbore, ktorý je nahraný do cloudu, TPA (third party auditor) overuje to, či je alebo nie je zabezpečený. Tento overovací proces je možné urobiť dvoma spôsobmi, a to priamou kontrolou a stiahnutím overenia.

Algoritmus pre verifikáciu TPA

Algoritmus pre verifikáciu je nasledovný (TPA používa Cc (dáta vlastníka) pre overenie integrity, v rámci algoritmu boli využité skratky uvedené v algoritme Eswarana (Eswaran a Abburu, 2012)).

Eswaranov algoritmus pre verifikáciu

```
begin
if overenieDokazu=priame then sprava:=priamyPristupNaSubor
else return(1,0):=overenieDokazu(Skluc)
/*vystup 1 (TRUE, pravda) ak integrita suboru je
verifikovana korektne,
inak 0 (FALSE, nepravda)
```

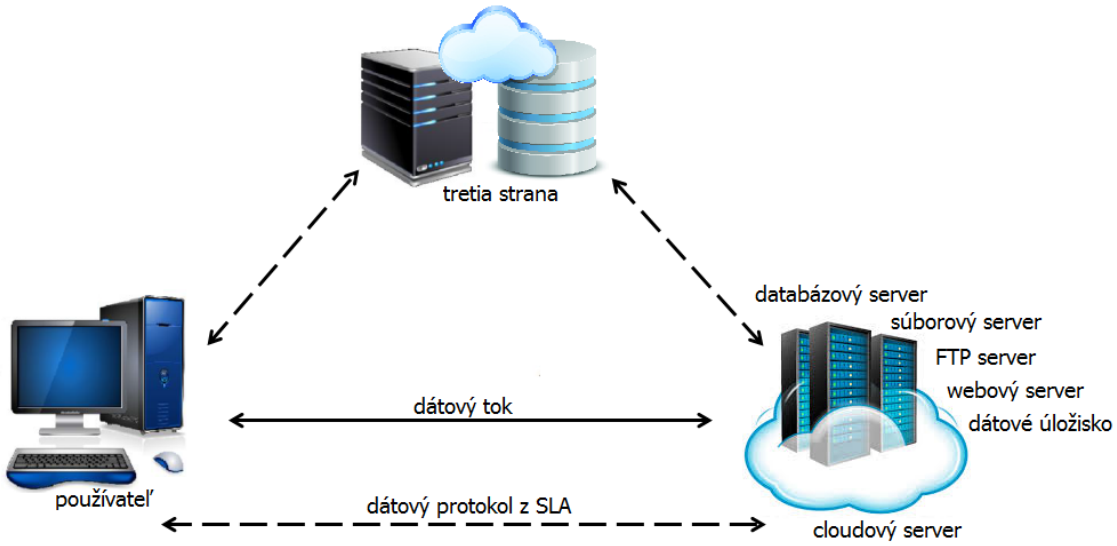
Algoritmus pre verifikáciu pracuje s dvomi subjektami (Yang, 2014):

- *používateľ* – používateľ zadáva požiadavku pre uloženie dát do cloudu, pričom môže využívať viacero cloudov pre všetky svoje výpočty na základe dát uložených na cloudovom servery,
- *cloudová služba (CSP)* – CSP obsahuje zdroje a odborné znalosti v oblasti budovania a správy distribuovaných úložísk cloudových serverov, vlastní, prevádzkuje a prenajíma systém zo strany auditora.

TPA má skúsenosti a schopnosti, ktoré používatelia nemôžu mať. Je dôveryhodný pre posúdenie, audit a vystavenie rizika služieb cloudu ako dátového úložiska v prospech používateľov na žiadosť osobitného subjektu používateľa. Tento algoritmus je považovaný za zaistenie bezpečnosti a schopnosti závislosti cloudového serveru uvedeného ako protivníkov model (Barsoum, 2013).

Protivník má záujem neustále kaziť dátové súbory koncového používateľa uložené na jednotlivých serveroch. Akonáhle nie je odozva serveru, protivník môže znečistiť pôvodné dátové súbory úpravou alebo zavedením vlastných podvodných údajov, aby zabránil načítaniu pôvodných dát používateľa (Yang, 2014).

Na obrázku 6 je znázornená navrhovaná architektúra siete využívajúca TPA pre ukladanie dát na cloudový server. Architektúra je postavená na predpoklade, keď používateľ má dáta už uložené na svojom lokálnom počítači. Preto musí byť zabezpečená správnosť a dostupnosť dátových súborov, ktoré sú uložené na distribuovaných cloudových serveroch. Jednou z kľúčových otázok je, ako účinne detekovať akúkoľvek neoprávnenú modifikáciu dát a korupciu kvôli kompromisu servera. (Cong, Sherman, Qian, Kui a Wenjing, 2013)



Obr. 6: Architektúra siete využívajúca TPA (Yang, 2014)

Z tohto dôvodu je prítomnosť TPA povinná pre posúdenie, audit a určenie rizikových služieb cloudu ako úložiska. Pre distribúciu súborov cez cloudové servery s ohľadom na verifikáciu teraz uvádzam základnú teóriu.

FEC (forward error correction) snímače sú zvyčajne parametrizované ako n-tice (m, k). Pre každú odchádzajúcu sekvenciu dátových paketov, celkom (M+K) dát a opravu chýb paketov, sú posielané cez kanál v režime kódovania k/m (Cong, Sherman, Qian, Kui a Wenjing, 2013). Redundantné informácie nemôžu byť generované a odoslané, pokiaľ sú k dispozícii pre odoslanie všetky dátové pakety (Velte, Velte a Elsenpeter, 2009)

V dôsledku toho *latencia zotavenia paketu* je určená rýchlosťou, pri ktorej odosielateľ prenáša dáta. Generovanie chybovej korekcie paketu ako dátového paketu na odosielateľa nie je dostupná voľba, aj keď rýchlosť prenosu dát v tomto kanáli je nízka, prijímač v sieti by mohol byť v prevádzke v takmer plnej kapacite s údajmi z iných odosielateľov a FEC je citlivý na nárazové straty (Yang, 2014).

Pre vykonávanie TPA je potrebné pripraviť *distribučný súbor*. Dáta sú rozdelené do dátového súboru F redundantne cez sadu d distribuovaných serverov. Transportná vrstva sa používa na určenie c redundancie parity vektory z R dátových vektorov ako cesta, ktorá pôvodné r dátové vektory môže rekonštruovať z akéhokoľvek r z r+c dát a parity vektorov. Vďaka tomu, že každý z r+c vektorov je na inom serveri, pôvodný dátový súbor môže prežiť poruchu každého c R+C serveru bez akejkoľvek straty dát, s priestorom nad hlavou C/R (Cong, Sherman, Qian, Kui a Wenjing, 2013). Nemodifikovaný r dátový súbor vektorov spolu s c paritami vektorov je distribuovaný cez r+c odlišné servery.

Koncový používateľ dostane kódovaný súbor vynásobením F s A (Yang, 2014)

pričom platí:

$$G = F \bullet A = (G(1), G(2), \ldots, G(m), G(m{+}1), \ldots, G(n)) = (F1, F2, \ldots, Fm, G(m{+}1), \ldots, G(n)), \quad (1)$$

kde F je aktuálny súbor a je odvodený od Vandermondovej matrice (matrica s podmienkami geometrického rastu kaž dého riadku). Pre názornosť uvádzam znázornenie Vandermondovej matrice.

Nech mám Vandermondovu matricu indexu 3, potom prvý blok obsahuje dátové pakety číslované *(0, 3, 6, …, (r-1)c)*, druhý blok je zložený z dátových paketov číslovaných *(1, 4, 7, …, ((r-1)c)1)* a tretí blok s dátovými paketmi s číslami *(2, 5, 8, …, ((r-1)c)2)*.

Používateľ si môže overiť nezávislého auditora tretej strany cloudového úložiska, keďže tieto informácie sú verejné (Cong, Sherman, Qian, Kui a Wenjing, 2013). Pre efektívnosť TPA, postup auditu by nemal priniesť žiadne nové zraniteľnosti voči ochrane osobných údajov používateľa. Podľa Yanga (Yang, 2014) TPA by nemalo určovať obsah používateľských dát prostredníctvom delegovaných dát auditu, avšak môže podporovať kontrolovanie treťou stranou o ochrane osobných údajov, zachovanie (Rocha, Abreu a Correia, 2013).

TPA audit by mal (Rocha, Abreu a Correia, 2013):

- nezavádzať žiadne nové zraniteľnosti,
- chrániť súkromné údaje zákazníkov,
- chrániť dôverné informácie poskytovateľa,
- výsledky auditu musia byť dôveryhodné.

Rocha (Rocha, Abreu a Correia, 2013) uvádza, že by sa malo vyhnúť predpisovaniu technológie, kedy používateľ deleguje zodpovednosť auditu na TPA (všetky atribúty potrebné pre overenie cloudového servera sú poslaté v zabezpečenom šifrovanom stave). Algoritmus TPA overuje cloudový server pre koncového používateľa a zdieľa výsledky správnosti záruky cloudového servera, na ktorého používateľ požadoval overenie.

Analýza bezpečnosti – spôsoby overovania integrity

Pre dosiahnutie *overenia integrity dát ukladaných do cloudu* a chybných lokalizácií dát využívam schému protokolu výzva – odpoveď.

Pre overenie integrity dát, je potrebné, aby platila nasledujúca definícia (Thuraisingham, 2013):

Ak je dátový súbor distribuovaný do cloudu, tak potom systém používateľa dopredu počíta určitý počet krátkodobých overovacích tokenov individuálneho vektora $G^j(j \in (1, \ldots, n))$, kde každý token predstavuje náhodnú podmnožinu dátových blokov, ktoré budú distribuované do rôznych cloudových serverov.

Pokiaľ chce koncový používateľ overiť správnosť uložených dát v cloude, tak napáda cloudové servery súborom náhodne generovaných blokov indexov (Ming, Shucheng, Kui, Wenjing a Thomas, 2013). Po prijatí výzvy, každý cloudový server vypočíta krátky podpis v priebehu uvedených blokov indexov a vráti ich používateľovi. Návratové hodnoty týchto podpisov by mali zodpovedať príslušným tokenom vopred vypočítaným na strane používateľa.

Nech používateľ chce napadnúť cloudový server t-krát s cieľom overenia zabezpečenia integrity dát, potom používateľ potrebuje dopredu vypočítať x overovacích tokenov pre každé $G^j(j \in (1, \ldots, n))$, pričom zmení kľúč k_{chal} a hlavnú permutáciu kľúča K_{PRP}.

Pre generovanie i_{th} tokenov pre server j, používateľ postupuje nasledovne (Ming, Shucheng, Kui, Wenjing a Thomas, 2013):

- vytvára deriváciu náhodnej hodnoty výzvy α_i a permutácie kľúča k^i_{prp} založené na K_{PRP},
- vypočíta sadu r náhodne vybraných indexov,
- ráta tokeny v^j_i pomocou náhodnej hodnoty výzvy α_i.

Po generovaní tokenov má používateľ možnosť buď manažovať vopred vypočítané tokeny lokálne, alebo ich zašifrované hodnoty uložené v cloude.

Hodnoty odozvy od servera pre každú výzvu (úlohu) určí nie len správnosť úložiska, ale taktiež obsah informácie o potenciálnych chybách dát. Procedúra i_{th} výzva – odpoveď pre overenie nad d servermi je nasledujúca (Thuraisingham, 2013):

- koncový používateľ odhalí permutačný kľúč ku každému serveru,
- server uloží vektor G^j agregácií, ktoré k-krát stanovia index permutácie kľúča v lineárnej kombinácii,
- po obdržaní lineárnej kombinácie zo všetkých serverov, používateľ vyberie slepú hodnotu,
- následne používateľ overuje, či prijaté hodnoty zostávajú platné kódovým slovom určenom v tajnej matici P.

Jeden zo spôsobov overovania integrity súboru dát je založený na *hashovacích hodnotách* (Hayes, 2008). Hash hodnota je odvodená tým, že kondenzuje súbor dát do jednej jedinečnej hodnoty formou vopred stanoveného algoritmu (Winkler, 2011). Vzhľadom k tomu, hash hodnota je odvodená od pôvodných dát samostatne. V prípade, že dve hash hodnoty nie sú zhodné, je to ukazovateľ toho, že aspoň jedna z oboch kópií bola buď zmenená alebo po škodená (Erl, Puttini a Mahmood, 2013).

Pri integrite dát je dôležité sa uistiť, že poskytovateľ poskytuje možnosť overiť hodnotu hash dát a porovnať ho s hash hodnotou druhej kópie dát, bez ohľadu na to, kde je uložená kópia (Mather, Kumaraswamy a Latif, 2009). Monitorovanie dát ručne by bolo veľmi obtiažne, a preto sa vyvinuli nástroje pre kontrolu dát.

Kým aktívny archív je jednou z metód monitorovania integrity dát, zostáva kritická potreba široko adoptovaného štandardného protokolu cloudu, ktorý podporuje integritu sledovanie a interoperability (Rhoton, Clercg a Graves, 2013). Vzhľadom k tomu, že nie všetky dátové centrá majú homogénne vybavenie, ani nemajú nevyhnutne homogénnu hostingovú infraštruktúru cloudu, interoperabilita medzi rôznymi úložnými zariadeniami je zásadná (Marsh, 2011).

Cloud Data Management Interface (CDMI) štandard bol navrhnutý v roku 2010 Industry Storage Networking Association (SNIA). CDMI-kompatibilný systém môže požadovať iný kompatibilný CDMI systém pre určenie hash hodnoty objektu, ktorá potvrdzuje, že dve kópie dát sú stále rovnaké (Hoff, Mogull a Balding, 2013). Tým, sledovanie integrity primárnej kópie dát so záložnou kópiou môže firma jednoducho overiť, a tak zistiť, či kópia dát uložených v cloude nebola po škodená. Ako často tieto dátové sady musia byť monitorované, môže byť určené hodnotou dát. Priemyselné štandardy, ako je CDMI, nie len zaisťujú interoperabilitu medzi kompatibilnými heterogénnymi systémami, ale tiež poskytujú pohodlný mechanizmus pre monitorovanie integrity dát (Marsh, 2011).

Verifikácia integrity dát pre redundantné servery

Riešenie integrity dát v cloud computingu súvisí s využitím cloudu ako úložiska. Pre vyššiu bezpečnosť uložených dát v cloude sa využíva redundancia, a tak vzniká problém ako riešiť overenie integrity dát pri redundantných/obnoviteľných serveroch (Luhman, 2013). Pre zvýšenie stupňa škálovateľnosti, dostupnosti a udržateľnosti niektorí koncoví klienti cloudu požadujú replikáciu dát na viacerých serveroch prepojených s hlavným dátovým centrom (Pearson a Yee, 2013). Zvyšujúce množstvo kópií dát predstavuje otázku pre poskytovateľov cloud. Riešenie tejto otázky načrtol Barsoum (Barsoum, 2013). V rámci zostavovania riešenia bezpečnosti dát bolo vychádzané z predpokladov a výsledkov výskumu.

Komponenty systému

Barsoumov (Barsoum, 2013) navrhnutý model ukladania dát pozostáva z troch celkov:

- *vlastník dát*, ktorým môže byť jedna osoba, alebo organizácia, ktorá spracováva citlivé dáta ukladané do cloudu,
- *poskytovateľ cloudových služieb*, ktorý manažuje cloudové servery a poskytuje navyšovanie úložného priestoru v rámci infraštruktúry pre uloženie dát vlastníka dát,
- *autorizovaní používatelia* sú nastavení vlastníci klientských účtov, ktorí majú práva k prístupu zmien dát.

Model ukladania dát používa pri verifikácii integrity dát prijatie mnohých praktických aplikácií (napríklad využitie e-health aplikácie). K takým aplikáciám sú zaradené finančné, vedecké a vzdelávacie aplikácie, ktoré majú zhodné nastavenie.

Nakoľko model pracuje s dátami, je jeho návrh zameraný na citlivý archív, ktorý je základom v mnohých aplikáciách ako sú digitálne knižnice a vedecké zdroje. Dáta predstavujú objekt, ktorý sa nefrekventovane mení, z čoho vyplýva hrozba v statickom stave (úložisko).

Redundancia dát

Pre dosiahnutie *redundancie dát* využívam Barsoumov model, kde formovač je jednoduchá cesta, ktorá môže byť použitá pre mnohé úložiská, pre dátový súbor s veľkosťou |F| bitov a nákladovo výhodné skladovanie pre n kópií nad cloudovými servermi je n|F| bitov. Vo vymazávacích kódoch je súbor delený na m blokov a l zakódovaných blokov vstupov pričom platí, že l je vačšie ako m. Zakódované bloky sú uložené v l odlišných serveroch, pričom platí jeden kódovaný blok na server pre predchádzanie zlyhania všetkých blokov a veľkosť úložiska (|F|/m)l bitov. Pôvodný súbor môže byť rekonštruovaný z akýchkoľvek blokov m výstupov z l serverov.

Poskytovateľ cloudu využíva pri redundancii vymazávanie kódu, čím dosiahne menšie skladovacie náklady, avšak duplikovanie dátového súboru naprieč viacerých serverov dosahuje škálovateľnosť, pri ktorej ak počet používateľov rastie, potom používateľ s viacerými dátovými kópiami v priebehu času dosahuje určitú hranicu odcudzenia (Gsoedl, 2011). Z tohto dôvodu vyplýva problém s riešením škálovateľnosti, keďže to je základná požiadavka koncového používateľa využívajúceho technológiu cloud computingu.

Súbor, ktorý je duplikovaný a uložený strategicky na niekoľkých serveroch (z lokálneho hľadiska ide o rôzne geografické lokácie), môže pomôcť redukovať prístupový čas a cenu za komunikáciu pre používateľa. Na druhej strane pri odpovedi požiadavky pristupovať k dátam cez jednoduchý kódovací systém, má poskytovateľ cloudu možnosť pristupovať k m serverom určeným na rekonštrukciu pôvodného dátového súboru. Je dôležité v tomto kroku zohľadňovať, že navyšovanie časových nákladov (latencia siete a výpočtový čas pre dekódovanie dátových blokov) nastáva na strane poskytovateľa cloudu.

Outsourcing a sprístupnenie dát

Nech vlastník dát má súbor F zložený z m blokov, potom poskytovateľ cloudu ponúka pre uloženie n kópii (F_1, F_2, ..., F_n) súboru vlastníka dát niekoľko odlišných serverov ako prevenciu pred stratou všetkých kópií. Počet kópií závisí na štruktúre dát. Viaceré kópie sú potrebné pre kritické dáta, ktoré nie je možné ľahko reprodukovať a ukladať s dodržaním najvyššieho stupňa škálovateľnosti. Tieto kritické dáta by mali byť replikované na viaceré servery prepojené s viacerými dátovými centrami. Na druhej strane nekritické reprodukovateľné dáta sú uložené na nižšej úrovni redundancie. (Martel, Nuckolls, Devanbu, Gertz, Kwong a Stubblebine, 2001)

Pre utajenie dát vlastník šifruje svoje dáta pred outsourcingom zo strany poskytovateľa cloudu (Singh a Liu, 2008). Autorizovaný používateľ outsourcingovaných dát zasiela požiadavku na poskytovateľa a prijíma kópiu súboru v šifrovanom formáte, ktorý môže byť dešifrovaný použitím tajného kľúča zdieľaného s vlastníkom dát (Singh a Liu, 2008). Na základe použitia mechanizmu vyrovnania záťaže na strane poskytovateľa pre manažovanie práce na serveroch je požiadavka prístupu

k dátam riadená serverom s najnižším preťažením, a teda autorizovaný používateľ nepozná, ktorú kópiu dát prijal. Popísaná interakcia medzi vlastníkom dát a autorizovaným používateľom pre autentifikáciu svojich identít a zdieľaní tajných kľúčov je považovaná za kompletnú, avšak nie je zahrnutá v Barsoumovom modeli.

Zhrnutie podkapitoly

Integrita dát je jednou z hlavných podmienok riešenia bezpečnosti dát v cloud computingu. Pre monitorovanie integrity dát je dôležité zohľadňovať poškodenie dát, ku ktorému môže dôjsť v rámci akejkoľvek úrovni uloženia v úložisku. Výsledné metadáta z poškodenia sú výsledkom bit root, deduplikácie, regulátora poruchy a ďalších uvedených možností.

Pre riešenie integrity dát v cloud computingu v rámci vlastnej práce využívam znalosti získané z protokolu o dohode jednotlivých úrovní služieb, protokolu o vyňatí, protokolu založenom na vkladaní náhodného strážcu v dátovom súbore. Pre verifikáciu integrity dát využívam TPA a verifikáciu integrity dát pre redundantné servery podľa Barsouma. Barsoumov model sa zameriava na riešenie redundancie dát, komponenty systému, outsourcing a sprístupnenie dát. Jeho výskum avšak neposkytuje hlbšie znalosti z hľadiska implementácie cloud computingu v podnikovom a univerzitnom prostredí. Bližší pohľad na riešenie predstavuje splnenie cieľa dizertačnej práce.

2.5 Cloud computing v podnikovom a univerzitnom prostredí

Technológia cloudu je využívaná v rôznych pracovných prostrediach. Cloud computing poskytuje vysokú škálovateľnosť, a tak jeho využitie ako úložiska môže byť vykonávané v akomkoľvek prostredí pomocou dostupných informačných technológií. Z charakteristiky prostredia cloudu vyplýva, že jedno dátové úložisko môžu využívať viacerí používatelia. Používateľ na Internete môže komunikovať s mnohými servermi naraz a tieto servery si navzájom vymieňajú informácie (Hayes, 2008). Zdieľanie informácií v reálnom čase medzi používateľmi poskytuje zlepšenie efektivity práce.

Dnešné cloudové platformy, ako napríklad Microsoft a Google poskytujú zdarma služby študentom a zamestnancom vo vzdelávacích inštitúciách, ktoré zahŕňajú e-mail, zoznamy kontaktov, kalendár, ukladanie dokumentov, vytváranie a zdieľanie dokumentov a schopnosť vytvárať webové stránky (Sclater, 2009). Avšak, služby cloud computing môže poskytnúť aj samostatná univerzita s možnosťou naďalej využívať nový vývoj v oblasti IT technológií za prijateľné náklady.

Do budúcna je vysoko pravdepodobné, že cloud sa stane východiskovou technológiou aj pre malé a stredné podniky, ako aj vzdelávacie inštitúcie. Britské Národné výpočtové centrum (NCC) odhaduje, že malé a stredné podniky môžu znížiť celkové náklady na vlastníctvo technológie využívajúce hostované riešenie (Microsoft, 2009). Nabil (Nabil, 2010) uvádza, že vedenie univerzity by malo identifikovať a vy-

užívať nové technológie, ktoré sú nákladovo efektívne, a tak sa snažia o čo najširší a spravodlivý prístup k technológii pre študentov a zamestnancov.

Pre určenie vhodnosti cloudu na vysokých školách som sumarizovala predchádzajúce štúdie. Využitie cloud computingu v škole tvorí 4 percentá z celkového využitia cloudu v iných odvetviach (najväčšie využitie je v oblasti finančných služieb a riadenia) (Tuncay, 2010). Cloudová škálovateľná inteligentná infraštruktúra predstavuje rozumné riešenie pre verejné služby, inteligentné dátové centrá, všade prítomnú výpočtovú techniku, automatizáciu, virtualizáciu a siete (Klein a Kaefer, 2008).

Študenti na univerzite používajú rôzne možnosti Internetu, ako je napríklad zdieľanie dokumentov, videá, prezentácie, softvér, komunikácia prostredníctvom e-mailu, zasielanie upozornení a podobne. Keďže ku prístupu do cloudu stačí webový prehliadač, považujem cloud za ideálny pre pracujúcich akademikov ako aj študentov (Lijun, Chan a Tse, 2008). Infraštruktúra cloud computing urýchlila prijatie rôznych technologických inovácií v akademickom prostredí a jeho zariadenie a zdroje by mohli byť prístupné pre vysokých škôl na vyžiadanie.

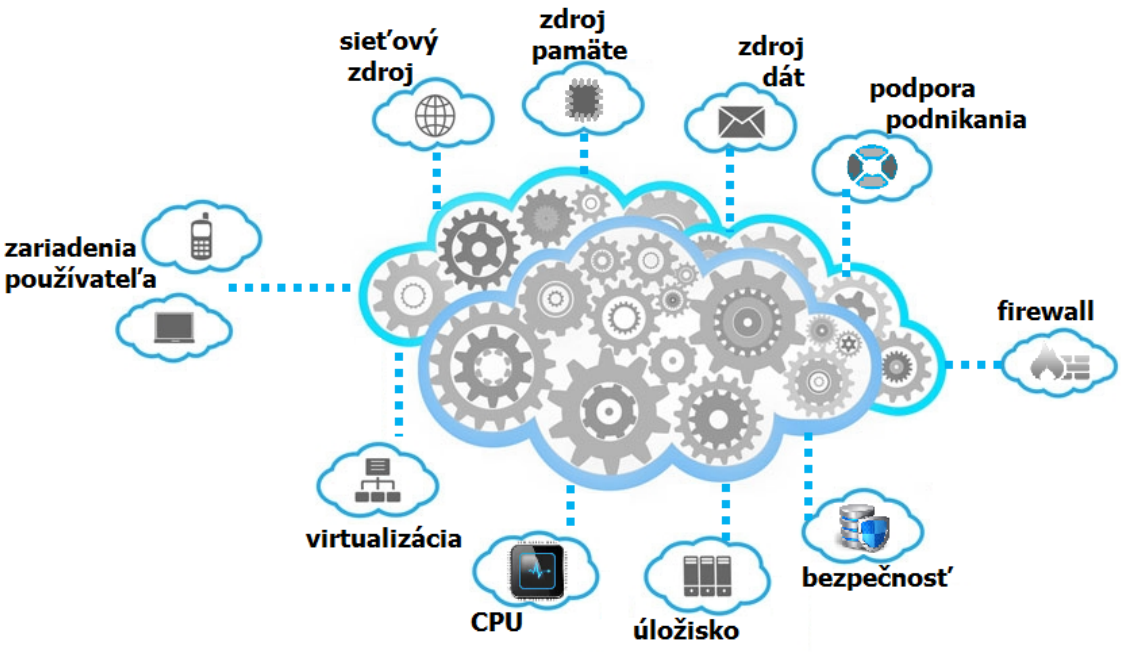
Praveena a Betsy (Praveena a Betsy, 2009) predstavili komplexný úvod do používania cloudu na vysokých školách. Delic a Riley (Delic a Riley, 2009) hodnotia súčasný stav vzdelávacích inštitúcií ako nutnosť premeniť infraštruktúru na globálnejšiu, spoľahlivu a efektívnejšiu, a to pomocou využitia cloud computingu. Vzdelávacie inštitúcie a univerzity vždy vyžadujú upgradovanie svojho softvéru a IT hardvéru, aby takto prilákali študentov a udržali krok s rýchlym vývojom v oblasti informačných technológií. Cloud computing môže poskytnúť týmto inštitúciám prostriedky na dosiahnutie týchto ambícií za ceny, ktoré si môžu dovoliť. Okrem toho, presun zodpovednosti na externých poskytovateľov pre správu niektorých aspektov ich softvéru a hardvéru infraštruktúry vedú k úsporám nákladov vzhľadom na prácu.

Tuncayov model infraštruktúry univerzitného cloudu

Tuncay (Tuncay, 2010) vytvoril model (Obrázok 7), ktorý sa snaží vyhovieť potrebám administratívnych pracovníkov (študentské záležitosti, financie a účtovníctvo, nákup a verejné obstarávania) a vzdelávania, odbornej prípravy a výskumu v súvislosti s potrebami študentov a akademických pracovníkov, najmä vo vzdelávacích inštitúciách. Tento model je založený na cloudovej infraštruktúre, ktorá bola rozdelená do blokov: používateľ, sieťové úložiská, virtualizácia, procesor, ukladanie dát, zabezpečenie kontinuity podnikania a brána firewall. (Priščáková a Rábová, 2013)

Bloky modelu vedú k zlepšeniu možnosti dolovania dát a hľadania ich obsahu. Z pohľadu študenta, model je konštruovaný tak, že neobmedzuje predmety alebo školy a obsah sa dynamicky mení v pravidelných intervaloch. Používateľ cloudu v tomto prípade je spojený s komerčnými službami tretích strán k vytvoreniu nových aplikácií.

Najdôležitejším rysom rôznych aplikácií, ktoré ponúka cloud je ich dostupnosť a škálovateľnosť (Tuncay, 2010). Používateľsky prívetivé rozhranie cloudových ap-



Obr. 7: Tuncayov model infraštruktúry univerzitného cloudu (Tuncay, 2010)

likácií umožní koncovým používateľom úspešne rozšíriť svoje výpočtové prostredie. Platforma plánovaná na základe cloudu poskytuje, že obsah aplikácie je skôr ako sa aplikácie ocitajú v centre (Erikson, Spence, Rhodes, Banks, Rutherford a Simpson, 2009). Obsah cloudu (vedecké a sociálne subjekty, umenie, názory, učebnice, encyklopédie) je riadený poskytovateľmi služieb a je používateľom k dispozícii vždy, keď o to požiadajú (Tuncay, 2010).

K vylepšeným technikám dolovania dát slúži filter, ktorý nachádza požadovaný obsah s cieľom pomôcť študentom. Cieľom študenta práce je neobmedzený prístup na kurzy alebo školy, a preto by mal byť existujúci obsah dynamicky menený a v určitých intervaloch (Tuncay, 2010). Vlastné služby sú kombinované s komerčnými službami tretej strany k vytvoreniu nových aplikácií (Tuncay, 2010).

2.6 Zhrnutie kapitoly

Ukladanie dát prebieha na základe redundancie, čím sa dosiahne určitý stupeň zvýšenia bezpečnosti. K najjednoduchším metódam zabezpečenia patrí autorizácia (prihlásenie na základe mena a hesla) používateľa. Pre vyššiu bezpečnosť dát je vhodnejšie využívať šifrovanie dát a priradenie autentizačného kódu pre dáta. Pre šifrovanie a zabezpečenie prenosu na strane klienta sa využijú technológie typu SSL.

Vzhľadom na verejný cloud je dôležité si uvedomiť, že s integritou dát závisí aj pôvod dát. Integrita dát sa vzťahuje na dáta, ktoré neboli zmenené neautorizovaným prístupom alebo neautorizovanou osobou. Pôvodom myslíme nie iba to, že dáta

podliehajú integrite, ale taktiež aj výpočtový výkon, teda dáta sú presne vypočítané (Mather, Kumaraswamy a Latif, 2009).

Napriek uvedeným mínusom je dôležité povedať, že nemôžeme cloud považovať za nevhodné úložisko, ale môžeme skôr povedať, že pri vyšetrovaní a vykonávaní cloudových stratégií existuje viac faktorov výberu, ako len náklady na každý uložený gigabajt. Ukladanie dát do cloudu ponúka mnoho výhod pre firmy všetkých veľkostí. Čo cloud však neponúka, je eliminácia potreby inteligentnej stratégie ukladania dát. Bez ohľadu na to, ako alebo kde sú údaje uložené, je absolútne nevyhnutné, aby sa firma ubezpečila, že budú dáta prístupné v akomkoľvek prípade. Na toto uistenie práve slúži sledovanie integrity dát a overovanie.

Z uvedenej literárnej rešerše vyplýva, že neexistuje komplexné riešenie zvýšenia bezpečnosti dát ukladaných do cloudu. Z tohto dôvodu som sa rozhodla pre stanovenie metodiky a jej verifikovanie pri implementácii v podnikovom a univerzitnom prostredí.

3 Riešenie problematiky

Riešenie problematiky vyplýva z uvedených teoretických východísk, vymedzenia riešených problémov, vlastného návrhu riešenia a výsledkov jeho testovania, ako aj stanovenia metodiky pre zvýšenie bezpečnosti dát uložených v cloude.

Štruktúra kapitoly je rozdelená do troch hlavných celkov, a to stanovenie návrhu riešenia (vytvorenie modelu), testovanie modelu spojené s formalizáciou a verifikáciou metodiky a návrh riešenia dostupnosti. Výskumná časť dizertačnej práce prebiehala v Mendelovej univerzite v Brne (z pohľadu implementácie cloudu v akademickom prostredí) a v strednej firme (z pohľadu implementácie cloudu v podnikovom prostredí), aj keď pre zvýšenie relevantnosti bola nadviazaná spolupracovala s viacerými firmami (Forpsi, Vema, Wedos).

Pre formalizáciu a verifikáciu navrhnutej metodiky boli využité 3 typy formalizácie: modelovanie systému s využití UML diagramov, Petriho siete a nedeterministický konečný automat.

3.1 Model zvýšenia bezpečnosti dát uložených v cloud computingu

Pre zjednodušenie a definovanie metodického rámcu boli použité diagramy jazyku UML: diagram prípadu použitia, sekvenčný diagram, diagram aktivít a diagram tried.

Bezpečnostné moduly

Nakoľko navrhnutý model zvýšenia bezpečnosti dát uložených v cloud computingu vychádza z teoretických východísk, bolo potrebné pred samotnou realizáciou modelu zaviesť zovšeobecnie dostupných informácií o bezpečnosti dát uložených v cloude. V rámci metodiky a jej súboru predpokladov a praviel pre bezpečnost boli definované komplexné celky, ktoré ovplyvňujú a charakterizujú životný cyklus dát uložených v cloude. (Prišťáková a Rábová, 2013)

Integrita a dôvernosť dát

Pokiaľ sa firma spolieha na poskytovateľa komerčných služieb pre služby prenosu dát ako komoditných položiek, než ako plne spravovať službu, môže byť oveľa ťažšie získať záruky týkajúce sa vykonávania bezpečnostných kontrol pre integritu a dôvernosť prenášaných dát. Ak je to neuskutočniteľné alebo nepraktické získať potrebné bezpečnostné kontroly a záruky účinnosti kontroly prostredníctvom vhodných zmlúv (kontraktov), podnik vykonáva vhodné kompenzačné bezpečnostné kontroly alebo uvedomelo pripúšťa ďalšie riziko.

Pre dodržanie integrity dát boli využité publikácie špecifikujúce jednotlivé obmedzenia. *NIST špeciálna publikácia 800-52* poskytuje návod na ochranu prenosu integrity a dôvernosti pomocou protokolu *Transport Layer Security*(TLS). *NIST špeciálna publikácia 800-77* poskytuje návod na ochranu integrity a dôvernosti prenosu

pomocou protokolu *IPsec*. *NIST špeciálna publikácia 800-81* poskytuje usmernenia pre systém DNS (domain name system) – správa overenia a overenie neporušenosti. NSTISSI číslo 7003 obsahuje návod na používanie ochranných systémov distribúcie.

Základný problém uvedených obmedzení spočíva v rozdelení jednotlivých pravidiel, pričom sa pravidlá navzájom neovplyvňujú. Je dôležité, aby pravidlá spĺňali všetky podmienky zachovania integrity dát pri ukladaní. Uvedené publikácie nezahŕňajú Poynterove pravidlá, verifikačné algoritmy a doporučené rizikové opatrenia. Na základe týchto dôvodov je vytvorená v modeli situácia, kde firma (univerzita) používa šifrovacie mechanizmy rozpoznania zmien údajov počas prenosu a šifrovacie systémy pre zabránenie neoprávnenému zverejňovaniu informácií počas prenosu, pokiaľ nie sú inak chránené alternatívnymi fyzickými opatreniami. Vylepšenie by mohlo spočívať vo vytvorení chránených distribučných systémov.

Vstupné dáta

Riadenie životného cyklu informácií zabezpečuje údaje ako sú klasifikácia, uloženie, používanie a likvidovanie na základe práv a regulačných obchodných požiadaviek. Tieto údaje sú dôležité pre klasifikáciu dát uložených v cloude, nakoľko determinovanie klasifikačných stupňov uložených dát predstavuje nové možnosti zabezpečenia dát. Každému klasifikačnému stupňu je priradený stupeň ochrany dát, ktorý zahŕňa rozhodnutie o výbere šifrovacieho systému a priradenie hashovacej hodnoty (prípadne opačná varianta).

Monitorovanie bezpečnosti

Firma (univerzita) sleduje bezpečnostné kontroly v informačnom systéme priebežne. Nepretržité *monitorovanie činnosti* zahŕňa riadenie konfigurácie a kontrolných informácií súčastí systému, bezpečnostné analýzy vplyvom zmien systému, priebežné hodnotenia bezpečnostných kontrol a podávanie správ o stave. Podnik posudzuje všetky bezpečnostné kontroly v informačnom systéme počas počiatočnej bezpečnostnej akreditáciu. Po počiatočnej akreditácii a v súlade s politikou OMB (office of management and budget), firma hodnotí podmnožinu kontrol ročne počas nepretržitého monitorovania. V prípade univerzitného prostredia sa jedná o menej časté hodnotenie z dôvodu nepredpokladaných zásahov do informačného systému v priebehu niekoľkých akademických období.

Výber vhodných podmnožín bezpečnostných kontrol je založený na:

- FIPS (federal information processing standards) 199 – kategorizácia bezpečnosti informačného systému,
- špecifické bezpečnostné kontroly na ochranu informačného systému vybraných a pracujúcich používateľských účtov firmy,
- úroveň zabezpečenia, dôvody, ktoré firma musí mať pri určovaní efektívnosti bezpečnosti kontroly v informačnom systéme. Spoločnosť zavádza kritériá výberu a následne vyberie podmnožinu bezpečnostných kontrol použitých v rámci informačného systému pre posudzovanie.

Organizácia taktiež stanovuje časový plán kontroly monitorovania s cieľom zabezpečiť adekvátne dosiahnuté pokrytie. Ide o bezpečnostné kontroly, ktoré sú rozhodujúce pre ochranu informačného systému alebo malé hodnotenia najmenej raz ročne. Všetky ostatné ovládacie prvky sú posudzované aspoň raz počas *akreditácie informačného systému*. Organizácie môžu používať hodnotenie aktuálnych výsledkov získaných počas nepretržitého ročného monitorovania FISMA (federal information security management act) posúdením povinností. Tento ovládací prvok úzko súvisí a navzájom sa podporuje s činnosťami požadovanými pri monitorovaní zmien konfigurácie do informačného systému.

Efektívne priebežné monitorovanie programom vedie priebežné aktualizácie bezpečnostného plánu informácie systému, zabezpečenia hodnotiacej správy, plán činností a míľniky. Prísne a dobre vykonaný kontinuálny monitorovací proces výrazne znižuje úroveň úsilie potrebného pre reakreditáciu informačného systému.

Pr monitorovanie bezpečnosti sa využívajú tieto publikácie. *NIST špeciálna publikácia 800-37* poskytuje návod na kontinuálny monitorovací proces. *NIST špeciálna publikácia 800-53A* poskytuje návod na posúdenie bezpečnostných kontrol. Pre vykonávanie monitorovania bezpečnosti firma zamestnáva externého certifikovaného auditora alebo certifikovaný tím pre priebežné sledovanie bezpečnostných kontrol v informačnom systéme.

Zlepšenie monitorovania je možné dosiahnuť rozšírením a maximalizovaním hodnôt prebiehajúcich posúdením bezpečnostných kontrol počas procesu nepretržitého monitorovania. Nezávislý certifikovaný agent alebo tím posúdi všetky bezpečnostné kontroly počas nasadenia informačného systému.

Klientský modul

Klientský modul odkazuje na koncového používateľa, nakoľko cieľom modulu je stanoviť primerané kontroly, ktoré by sa mali uplatniť pre všetkých klientov, ktorí spracovávajú informácie alebo sprostredkujú prístup iných informačných systémov. Tento modul odkazuje na celú architektúru.

Riadenie účtov

Firma spravuje informácie systému účtov, vrátane vytvárania, aktivácie, úpravy, revízie, vypnutia a odstránenia účtov. *Riadenie účtov* zahŕňa identifikáciu typov kont (individuálne, skupiny a systém), vytvorenie podmienok pre členstvo v skupine a priradenie súvisiacich povolení. Podnik určuje oprávnených používateľov informačného systému a určuje prístupové práva.

Firma poskytuje prístup založený na základe potreby, požiadavky, ktorá je určená pridelenými služobnými povinnosťami a spĺňa všetky kritériá bezpečnosti personálu, a taktiež ide aj o určené využitie systému. Podnik má disponovať podanými žiadosťami o zriadenie účtu v informačnom systém, a taktiež súhrnom takýchto schválených žiadostí. Firma osobitne povolí a monitoruje využívanie pridelených a anonymných účtov, ako aj odstraňuje, zakáže alebo inak zabezpečuje prebytočné účty.

Správca používateľských účtov je upozornený, keď sú ukončené alebo prevedené kontá používateľov systému pridružené k iným kontám. Na podporu riadenia

účtov firma využíva dostupné mechanizmy (softvér). Informačný systém automaticky ukončí dočasné a núdzové účty po expirovaní priradeného časového obdobia pre každý typ účtu. Informačný systém automaticky vypne neaktívne účty po dosiahnutí definovaného časového obdobia. Podnik využíva automatizovaný softvér pre audit účtov - tvorbu, úpravu, vypnutie a ukončenie akcie, oznámenie pre príslušné osoby.

Riziká zabezpečenia

Firma vyvíja, rozširuje, pravidelne zadáva a aktualizuje opatrenia pri rizikách zabezpečenia. Podnik posudzuje formálne zdokumentovanú *politiku rizík*, ktorá rieši, či je potrebný povolený rozsah subjektov, zodpovednosti, angažovanosti manažmentu, koordinácie a podobne. V rámci zabezpečovania rizík vystupujú aj formálne zdokumentované postupy na uľahčenie vykonávania politiky posudzovania rizika a súvisiace kontroly posudzovania rizika.

Citlivé dáta

Firma priradí prístup k citlivým dátam na základe roly používateľa určenej pomocou riadenia účtov. V rámci tohto modulu sa aj aktualizujú posúdené riziká, nakoľko zmena v priradení úrovne zabezpečenia sa odzrkadlí aj na posúdených rizikách.

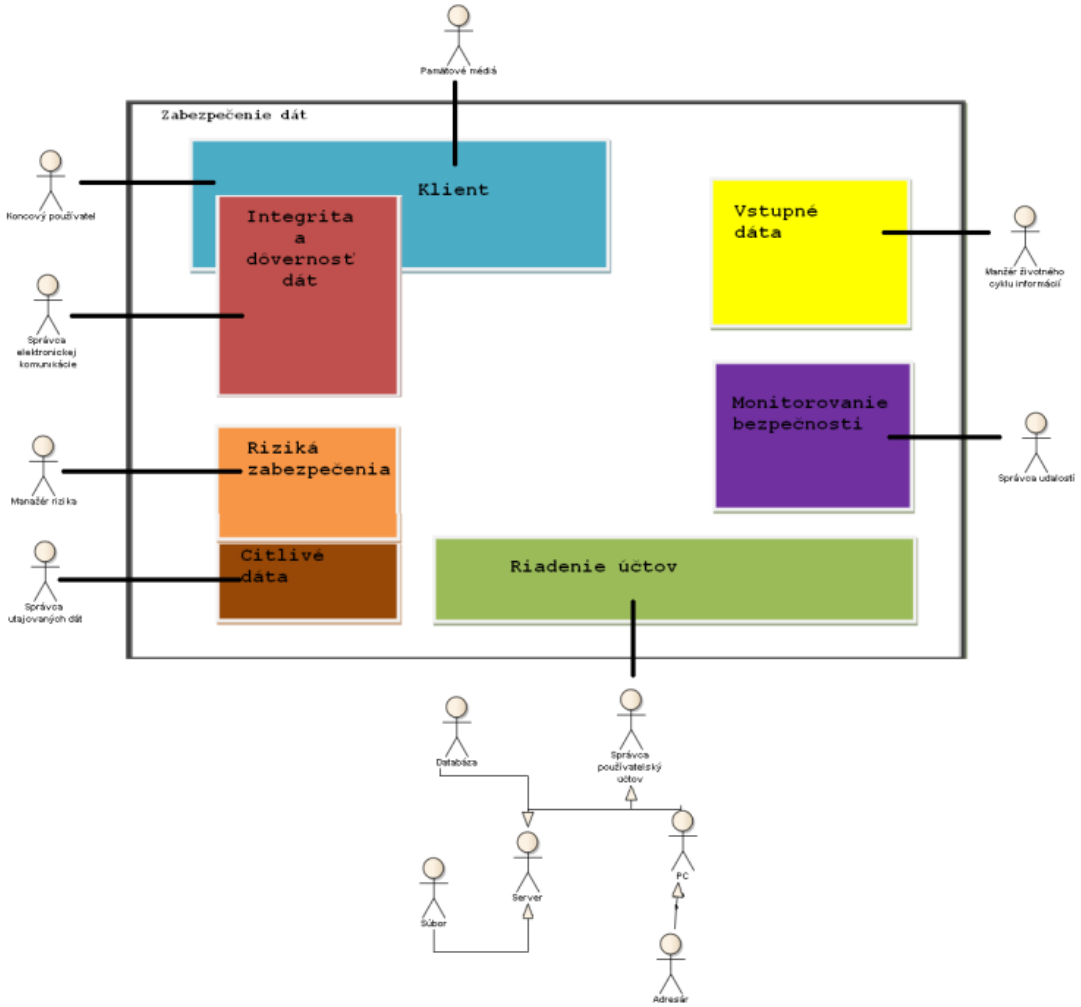
Na obrázku 8 sú znázornené jednotlivé elementy zabezpečenia dát, ktoré boli opísané v predchádzajúcich bodoch. Obrázok zahrňuje stanovenie jednotlivých aktérov a ich priradenie k modulom. Tento diagram predstavuje hrubý náčrt modelu zabezpečenia dát v podnikovom a univerzitnom prostredí. Uvedený návrh riešenia z diagramu je špecifikovaný diagramom prípadu použitia v Prílohe A.

Model prípadu použitia navrhnutej metodiky

Diagram prípadu použitia (Príloha A) pozostáva z hlavných aktérov, ktorí sa podieľajú na zabezpečení dát. Dôležitým aktérom je práve zamestnanec firmy, ktorý s dátami pracuje – koncový používateľ. *Koncový používateľ* pracuje s dátami prostredníctvom klienta. Vyžaduje sa od neho, aby bol zaškolený do systému zabezpečenia dát, aby vedel základné informácie o zabezpečení údajov a poznal osobitné požiadavky pre citlivé informácie v obchodnom kontexte. Z pohľadu akademického prostredia je koncovým používateľom študent, akademický a technický pracovník.

Je dôležité poznamenať, že pre prihlásenie koncového používateľa do informačného systému je potrebná autentizácia používateľa, ktorá väčšinou spočíva v zadaní mena a hesla. Tieto jednotlivé prípady použitia daného aktéra sú zoskupené nie len v module klienta, ale aj v integrite a dôvernosti dát.

Pamäťové média slúžia primárne na ukladanie kópií dát. Pamäťovým médiom v tomto prípade rozumiem aj vytlačený dokument. Je dôležité, aby tieto médiá boli kontrolované, respektíve, aby sa nepoužívali vôbec, čím by sa zabránilo strate dôverných údajov spôsobených tlačou alebo kopírovaním na vymeniteľné médium. Pokiaľ je nevyhnutné použiť pamäťové médium, je vhodné zaviesť prevenciu pred



Obr. 8: Diagram modelu pre zvýšenie bezpečnosti dát v cloude

stratou údajov spôsobenú tlačou alebo kopírovaním v podobe kontroly cez prenášaný port.

Šifrovanie citlivých informácií spravuje manažér rizika. Manažér rizika pracuje s pamäťovými médiami, nakoľko na základe zostavenia politiky postupu pri riešení rizík povoľuje a zamedzuje manipuláciu pri ukladaní dát. Taktiež určuje rizikové procedúry, ktoré môžu nastať pri ukladaní údajov.

Správca udalostí má na starosti *monitorovanie bezpečnosti*. Správca utajovaných dát pracuje v rámci modelu citlivých dát, kde spolupracuje s manažérom rizika. K jeho hlavným činnostiam patrí priradenie úrovne zabezpečenia.

Správca používateľských účtov má hierarchickú štruktúru. Je to z toho dôvodu, že štruktúra sa odvíja od práce používateľa, vykonávanej práce pri riadení účtov, a zároveň stanovení jednotlivých privilégií a prístupových práv pre klientov. Bližší popis týchto aktérov je charakterizovaný spoločným diagramom prípadu použitia pre súbor aj databázu. Činnosti manažéra životného cyklu informácií sú definované prostredníctvom modulu vstupné dáta.

Diagram prípadov použitia uvedený v prílohe A je podrobnejšie popísaný pomocou rozšírených vzťahov include a extend (Príloha B). Z dôvodu zložitosti tohto diagramu pre využitie v rámcovej metodiky boli vyplývajúce väzby formalizované prostredníctvom kontingenčnej tabuľky(Príloha C). V rámci tabuľky sú farebné označení jednotliví aktéri. Stĺpce tabuľky tvoria moduly a riadky tabuľky tvoria jednotlivé prípady použitia.

Statický pohľad na navrhnutý model predstavuje diagram tried (Príloha C). Diagram tried pozostáva z týchto tried: Manazer rizika, Rizika, Spravca utajovanych dat, Oznacene udaje, Zabezpecene data, Hranica ochrany, Spravca elektronickej komunikacie, Pamatove media, Informacny tok vykonu, Externy informacny system, Vstupne data, Manazer zivotneho cyklu informacii, Zasifrovane data, Spravca udalosti, Monitorovane udalosti, Spravca pouzivatelskych uctov, PC, Adresar, Povolene zabezpecenia, Urovne zabezpecenia, Minimalne opravnenia, Klient, Subor, Server, Databaza, Uniky dat, Ochrana zabezpecenia osobnych udajov. (Priščáková a Salák, 2014)

V rámci stanovenia a verifikácie metodiky sú uvedené vzťahy medzi triedami. Uvedené podmienky jednotlivých väzieb medzi triedami určujú výslednú formalizovanú metodiku.

Väzba Klient – Subor

Každý klient má v rámci systému priradený jeden súbor. V súbore sa nachádzajú dáta, ktoré určujú povinnosti koncového používateľa, teda upresňujú akú prácu môže používateľ vykonávať s akými dátami. Povinnosti sú radené do typu povinností, keďže niektoré povinnosti sú bežné a druhé obsahujú vysoké riziká.

Väzba Klient – Vstupne data

Klient pracuje so vstupnými dátami. Z hľadiska bezpečnosti dát a povinností koncového používateľa je vhodné, aby konkrétne dáta spravoval iba jeden používateľ. Pri multispracovaní jedného typu vstupných dát viacerými klientmi by mohlo dôjsť k chybe z hľadiska správneho spracovania týchto dát.

Nesprávne spracovanie dát by sa neskôr odhalilo pri zabezpečení dát. Koncový používateľ môže v momente vykonávania práce spracovávať viaceré vstupné dáta, avšak môže nastať aj prípad, kedy nepracuje so vstupnými dátami, ale je prihlásený v systéme (napríklad telefonický rozhovor počas pracovnej doby, prestávka, odchod z pracoviska bez odhlásenia a podobne).

Väzba Klient – Databaza

Koncový používateľ sa do systému prihlasuje na základe mena a hesla. Tieto údaje sú uložené v jednej databáze používateľov. Teda tento vzťah vysvetľuje spôsob kontroly prihlasovacích údajov. V špecifickom prípade môže nastať situácia, že v databáze nebude zadaný ešte žiaden klient.

Väzba Server – Subor – Databaza

Triedy Subor a Databaza predsavujú časti triedy Server. Zavedením tohto vzťahu medzi triedami poukazujem na umiestnenie doteraz uvedeného súboru a databázy klientov. Trieda Server mi poskytuje informácie o umiestnení uvedených tried vo virtualizovanom prostredí, a taktiež možnosť kontrolovať miesto prihlásenia klienta.

Väzba Spravca pouzivatelsky uctov – Server – PC

Vzťah Spravca pouzivatelsky uctov – Server – PC vysvetľuje, kto má zabezpečuje správu serveru a fyzického počítača. Túto správu kontrolujem z dôvodu zvýšenia bezpečnosti dát pri práci s dátami. Na základe tejto správy viem určiť, kto pracuje s akými dátami, na akom mieste, aké sú možnosti spracovania dát v prípade jednotlivých klientov a podobne. Trieda PC mi slúži pre identifikáciu počítača v infraštruktúre firmy.

Väzba PC – Adresar

Koncový používateľ pracuje na počítači, v ktorom má niekoľko adresárov. Každý adresár má priradené určité povolené zabezpečenia z hľadiska ochrany dát. Z tohto vyplýva, že touto väzbou určím na akom počítači klient pracuje, a zároveň s akým adresárom.

Väzba Adresar – Povolene zabezpecenia

V predchádzajúcej väzbe bola uvedené podstata triedy Adresar. Táto trieda je dôležitá pre triedu Povolene zabezpecenia. Pre každý adresár je určená jedna možnosť zabezpečenia. Trieda Povolena zabezpecenia mi poskytuje informáciu, či je daný adresár chránený a ako je chránený. Dané zabezpečenie je priradené minimálne k jednému adresáru.

Väzba Povolene zabezpecenia – Urovne zabezpecenia

Trieda Povolene zabezpecenia obsahuje úroveň zabezpečenia dát. Úroveň zabezpečenia dát využívam pre rozdelenie dát do kategórií vzhľadom na citlivosť dát. K jednému typu zabezpečenia priraďujem jednu konkrétnu úroveň zabezpečenia dát.

Väzba Povolene zabezpecenia – Zasifrovane data

Dáta sa šifrujú na základe povolených zabezpečení, a preto môžu mať priradený iba jeden typ povolenia. Tento typ môže byť použitý pre viaceré zašifrované dáta.

Väzba Zasifrovane data – PC

Pre šifrovanie dát potrebujem vedieť viaceré informácie. Ako bolo uvedené, jednou z hlavných informácií je typ povoleného zabezpečenia. Táto väzba poukazuje na situáciu, keď pri šifrovaní chcem vedieť z akého počítača dáta pochádzajú. Táto situácia je výnimočná a nemusí nastať. Pravdaže, ak už táto situácia nastane, k zašifrovaným dátam je priradený iba jeden počítač.

Väzba Zasifrovane data – Vstupne data

Trieda Zasifrovane data potrebuje vstupné dáta. Konkrétne vstupné dáta môžu byť zašifrované len raz. Trieda Vstupne data poskytuje hlavné informácie pre triedu Zasifrovane data, avšak aby bolo možné vykonať šifrovanie, je potrebné zahrnúť aj vzťahy medzi ďalšími triedami.

Väzba Zasifrovane data – Oznacene udaje

Zašifrované dáta je potrebné označiť (priradím im hashovaciu hodnotu). Označením rozumiem spôsob priradenia jedinečnej hodnoty vzhľadom na vstupné dáta. Vďaka označeniu zaručujem zvýšenie integrity dát ukladaných do cloudu. Konkrétne zašifrované dáta majú priradené iba jedno označenie.

Väzba Oznacene udaje – Manazer zivotneho cyklu informacii

Manažér životného cyklu informácií sleduje beh vstupných dát v rámci ich životného cyklu v systéme. Z tohto dôvodu mu poskytuje možnosť požadovať zobrazenie označenia údajov. Manažér môže sledovať viaceré označené údaje, avšak jeden konkrétny typ označenia je prisúdený iba jednému konkrétnemu manažérovi. Týmto obmedzením zabránim možným únikom dát.

Väzba Oznacene udaje – Zabezpecene data

Označené údaje vytvárajú zabezpečené dáta, avšak pre kompletné zabezpečenie dát je ešte potrebná hranica ochrany dát. Jedno označenie tvorí iba jedno zabezpečenie dát (nutné z hľadiska dodržania integrity dát).

Väzba Oznacene udaje – Rizika

Pre každé označené dáta je potrebné určiť riziká a stanoviť bezpečnostnú politiku v prípade, že riziko nastane. Tým, že pre označené dáta určím dostupné riziká, vytváram možnosť rýchlej reakcie pri riešení rizika, ako aj určujem dôležitosť dát a možné úniky dát. Pre konkrétny označený údaj priradím jeden typ rizík, avšak tento typ rizík môže byť aplikovaný pre viaceré označené údaje.

Väzba Rizika – Manazer rizika

Riziká určuje a aktualizuje manažér rizika. Pre riziko je potrebné určiť bezpečnostnú politiku a bližšie popísať dané riziko. Tieto činnosti pre jedno riziko vykonáva iba jeden manažér rizika. V systéme môže nastať aj netypická situácia, kedy nie sú vstupy, a teda nie je potrebné určiť riziko. Manažér môže spracovávať viacero rizík, a preto je násobnosť pri triede Rizika neobmedzená.

Väzba Rizika – Spravca utajovanych dat

Riziká a bezpečnostnú politiku k rizikám dokáže ovplyvňovať aj správca utajovaných dát. Správca môže ovplyvniť viaceré riziká, avšak ten konkrétny záznam k riziku vytvára iba jeden správca.

Väzba Rizika – Hranica ochrany

Na základe určenia rizikových procedúr s dátami a bezpečnostnej politiky je potrebné stanoviť hranicu ochrany dát. Hranica ochrany dát je tvorená niekoľkými kategóriami. Hranica ochrany dát je vytvorená na základe triedy Rizika, a preto medzi triedami je kompozícia (trieda Rizika je komponent a trieda Hranica ochrany je celok). K jednému riziku je prisúdený iba jeden typ hranice ochrany, avšak jeden typ dokáže byť prisúdený k viacerým rizikám.

Väzba Hranica ochrany – Zabezpecene data

Zabezpečené dáta majú prisúdenú hranicu ochrany dát. Hranica ochrany dát mi bližšie určuje o aké zabezpečenie dát ide a ako sa mám k dátam správať v prípade, že nastane riziko. Konkrétny typ hranice ochrany je použitý pri viacerých zabezpečených dátach. Pre zabezpečené dáta určím iba jednu hranicu ochrany.

Väzba Hranica ochrany – Spravca elektronickej komunikacie

Keďže elektronickú komunikáciu riadi správca elektronickej komunikácie, je vhodné, aby dokázal prisudzovať hranicu ochrany pre určitú komunikáciu. Konkrétny typ hranice ochrany môže nastavovať iba jeden správca. Pri nastavení hranice pre komunikáciu je dôležité, aby správca mohol pracovať aj s viacerými typmi hranice.

Väzba Zabezpecene data – Pamatove media

Zabezpečené dáta môžu byť uložené na pamäťové médium. Jedny konkrétne zabezpečené dáta môžu byť uložené na viaceré pamäťové médiá, avšak môže nastať aj situácia kedy nie sú uložené na žiadne médium (napríklad prerušenie komunikácie, zrušenie požiadavky pre uloženie). Na pamäťovom médiu môže byť uložených viac zabezpečených dát, čo ale zvyšuje riziko odcudzenia citivých údajov.

Väzba Spravca elektronickej komunikacie – Informacny tok vykonu

Správca elektronickej komunikácie sleduje tok výkonu. Súčasne môže sledovať viacero tokov.

Väzba Spravca elektronickej komunikacie – Externy informacny system

Systém môže komunikovať s externým informačným systémom. Aby bolo zabránené možným únikom, bol prisúdený externému systému správca elektronickej komunikácie. Správca môže súčastne komunikovať s viacerými externými systémami. Vďaka triede Externy informacny system môžem určiť aké sú funkcie tohto systému pre môj systém.

Väzba Pamatove media – Externy informacny system

Externý informačný systém môže komunikovať s pamäťovými médiami. Táto situácia nie je nutná pre navrhnutý systém.

Väzba Pamatove media – Vstupne data

Vstupné dáta vznikajú z dát, ktoré sú uložené na pamäťovom médiu. Vstupné dáta môžu byť čerpané z viacerých zdrojov, pričom však viaceré zdroje vytvárajú len jeden typ vstupných dát.

Väzba Vstupne data – Manazer zivotneho cyklu informacii

Vstupné dáta ovplyvňuje manažér životného cyklu informácií, nakoľko jeho cieľom je sledovať životný cyklus dát. Manažér môže súčasne spravovať viacero vstupných dát, pričom jeden konkrétny typ vstupných dát môže riadiť iba jeden manažér.

Väzba Spravca utajovanych dat – Urovne zabezpecenia

S triedou Rizika bola uvedené aj triedu Spravca utajovanych dat. Táto trieda komunikuje s triedou Urovne zabezpecenia. Správca utajovaných dát priraďuje jednotlivé úrovne zabezpečenia, a taktiež bližšie špecifikuje ich popis. Správca spravuje minimálne jednu úroveň. Úroveň zabezpečenia môže popisovať iba jeden správca. Vyplýva to z dôvodu, že správca utajovaných dát pozná riziká práce s dátami a je oprávnený vhodné posúdiť úroveň bezpečnosti.

Väzba Spravca utajovanych dat – Ochrana zabezpecenia osobnych udajov

Tak ako majú byť chránené dáta, tak je potrebné dbať aj na chránenie osobných údajov klientov. Keďže pre utajovanie dát v systéme mám správcu, preto jeho trieda komunikuje s osobnými údajmi a určuje typ ochrany. Jeden správca spravuje viacero osobných údajov. Aby bola docielená identita kto konkrétne prisúdil danú ochranu konkrétnym osobným údajom, bol priradený ochrane zabezpečenia iba jeden správca.

Väzba Urovne zabezpecenia – Minimalne opravnenia

V predchádzajúcich odsekoch bola uvedená náplň práce správcu utajovaných dát. V rámci jeho úloh je aj určovanie úrovne zabezpečenia dát. Na základe prisúdenia úrovne zabezpečenia dát sa určujú minimálne oprávnenia pre prácu s dátami. Ku každej úrovni mám prisúdené iba jedny minimálne oprávnenia, a každé minimálne oprávnenie je viazané iba k jednej úrovni. Trieda Urovne zabezpecenia predstavuje zaradenie do hodnotového bezpečnostného systému.

Väzba Minimalne opravnenia – Subor

Na základe nastavenia minimálnych oprávnení pre klienta je vytvorený jeden súbor, ktorý obsahuje povinnosti koncového používateľa pri práci s dátami. Nastavené minimálne oprávnenia môžu byť naviazané k viacerým súborom, keďže viacero klientov môže vykonávať rovnaké operácie s dátami.

Väzba Ochrana zabezpecenia osobnych udajov – Databaza

Každý klient má okrem súboru s minimálnymi oprávneniami k práci s dátami aj svoj používateľský účet, na základe ktorého sa prihlasuje do systému. Prihlasovacie údaje, tak ako aj osobné údaje používateľa, sú uložené v databáze. Keďže táto databáza obsahuje citlivé údaje, je potrebné ich zabezpečiť. Pre bezpečnosť týchto dát je vytvorená trieda Ochrana zabezpecenia osobnych udajov, ktorá poskytuje spôsob zabezpečenia osobných údajov. Databáza využíva viacero typov ochrán, nakoľko údaje používateľa delím do viacerých kategórií (meno a priezvisko je zverejnené, a preto má nižšiu úroveň bezpečnosti, zatiaľ čo prihlasovacie údaje sú citlivé, a majú vyššiu úroveň bezpečnosti).

Väzba Databaza – Uniky dat

Trieda Uniky dat slúži pre možnosť kontrolovať únik dát vzhľadom na povolené činnosti používateľa systému. Únik nemusí nastať, alebo môže ich byť niekoľko v rámci jedného používateľského účtu.

Väzba Uniky dat – Monitorovane udalosti

Akákoľvek zmena v systéme, ktorá môže ohroziť bezpečnosť dát je monitorovaná. Preto triedu Monitorovane udalosti dávam ako celok a pripájam k nej komponenty. Trieda Monitorovane udalosti obsahuje aj vyskytnuté úniky dát zo strany používateľa. Z každého úniku vzniká jedna monitorovaná udalosť.

Väzba Monitorovane udalosti – Spravca pouzivatelskych uctov

Aby bola docielená komplexná kontrola a nadhľad nad správaním používateľa počas využívania používateľského účtu v systéme, boli vytvorené väzby medzi triedami Monitorovanie udalosti a Spravca pouzivatelskych uctov. Správca na základe monitorovania udalostí vykonáva patričné zmeny v rámci nastavenia povolenia používateľských účtov a podobne.

Väzba Monitorovanie udalosti – Databaza

Prihlasovacie údaje koncového používateľa sú časovo ohraničené. Aby nedošlo k úniku dát po expirovaní, prípadne po ukončení používateľského účtu, monitorujem udalosti v databáze. Monitorované udalosti sú vytvárané z dát databázy, a preto ide o kompozíciu. Môže nastať situácia, že v databáze budú viaceré zmeny.

Väzba Monitorovanie udalosti – Ochrana zabezpecenia osobnych udajov

Ďalšou monitorovanou udalosťou je ochrana zabezpečenia osobných údajov. V prípade, že nastane situácia úniku osobných dát používateľov, tak je potrebné kontrolovať nastavenú ochranu zabezpečenia. V riešení využívam niekoľko typov ochrany zabezpečenia. Každá udalosť je viazaná ku konkrétnemu typu.

Väzba Monitorovanie udalosti – Spravca udalosti

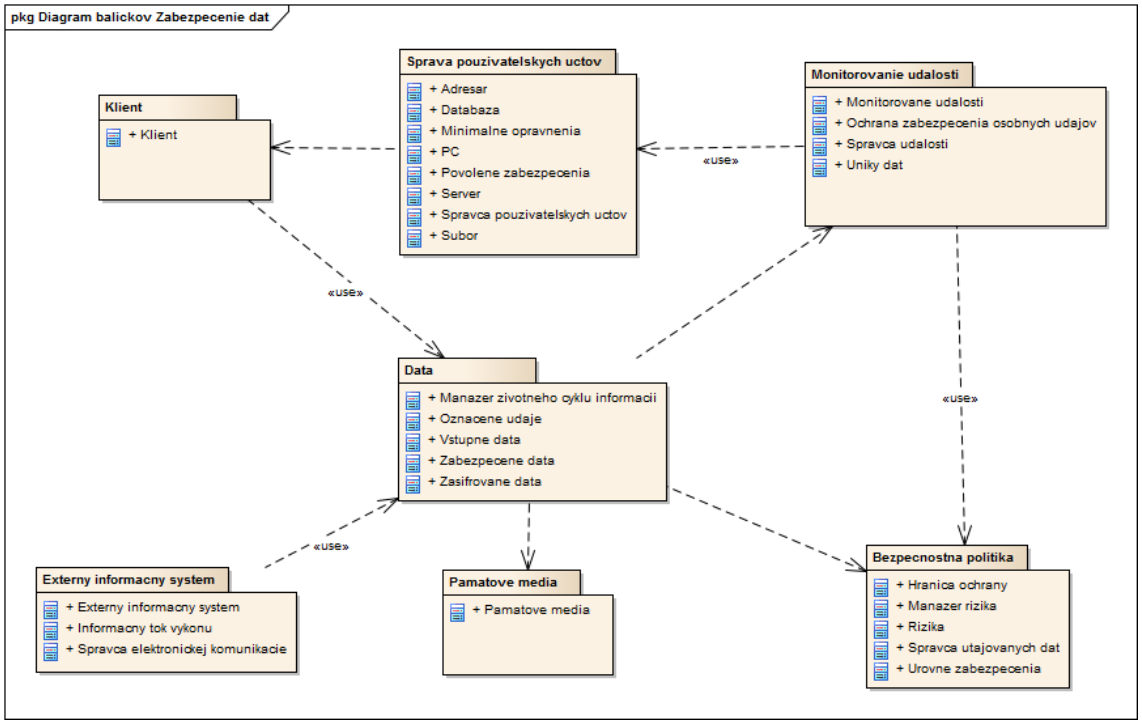
Každú monitorovanú udalosť sleduje správca udalostí. Okrem monitorovania môže udalosť aj vytvárať. Jednu udalosť do systému zadáva iba jeden správca, avšak správca môže súčasne monitorovať viacero udalostí (prípadne žiadnu, keďže systém si dokáže vytvárať udalosti sám, a taktiež ich dokáže riešiť).

Pre zapuzdrenie vytvoreného priestoru v modeli som využila diagram balíčkov. Cieľom balíčkov je vytvoriť hranice, ktoré určujú priestor, v rámci ktorého sú všetky názvy jedinečné. Všeobecne platí, že balíček je univerzálny mechanizmus usporiadania prvkov a diagramov do vzájomne sémantických skupín. Balíčkami som realizovala činnosti spojené s návrhom jednotiek pre súbežnú prácu, zoskupením sémanticky závislý prvkov, definovaním vnútorných hraníc modelu a podporou správy konfigurácie.

Z obrázku 9 vyplýva rozdelenie tried ako aj interakcia balíčkov. V nasledujúcich odsekoch sú definované vzťahy jednotlivých tried v rámci balíčkov.

Balíček Sprava pouzivatelskych uctov

Balíček Sprava pouzivatelskych uctov zahŕňa triedy, ktoré ovplyvňujú používateľský účet v rámci systému. Hlavnou triedou v balíčku je trieda Spravca pouzi-



Obr. 9: Diagram balíčkov navrhnutého modelu

vatelskych uctov. Informácie, ktoré správa v systéme dostáva, pochádzajú z dvoch zdrojov.

Prvým zdrojom je trieda Server. Úlohou tejto triedy je fyzická kontrola miesta pripojenia klienta do systému. Výstupy tejto procedúry zvyšujú bezpečnosť dát z hľadiska odcudzenia dát pre súkromné účely koncového používateľa. Na servery mám databázu a súbor. V databáze sú uložené prihlasovacie údaje klienta. V rámci tejto triedy mám procedúru pre kontrolu expirácie účtu. Touto procedúrou zabránim využívaniu používateľského účtu aj po ukončení práce vo firme (na univerzite).

Trieda Subor obsahuje informácie o povinnostiach používateľa a ich zaradení. Povinnosti používateľa predstavujú operácie, ktoré klient vykonáva v systéme, a taktiež s akými dátami. Typ povinnosti je určený na základe uvedených povinností používateľa. Procedúra Typ povinnosti zadeľuje jednotlivých klientov do určitých úrovní vzhľadom k práci v systéme.

Druhým zdrojom pre správcu je trieda PC. V tejto triede dokážem identifikovať počítač, na ktorom sa nachádzajú dáta, s ktorými používateľ pracuje. Identifikáciou počítača obmedzím možnosť odcudzenia dát klientom na iný počítač. Ak nie je počítač identifikovaný ako dostupný počítač z počítačov firmy (univerzity), práca v systéme sa ukončí.

Trieda Adresar slúži pre prácu s dátami. Pri práci s dátami koncový používateľ pracuje s adresármi, ktoré sú delené na základe bezpečnosti dát. Na každom počítači sú rozdelenia adresárov.

Balíček Data

Životný cyklus dát je obsiahnutý v balíčku Data. Tento cyklus riadi manažér životného cyklu informácií. Vstupné dáta (vstupom je manažér, externý informačný systém, pamäťové médium, dáta od používateľa) sú zašifrované. Po zašifrovaní je dátam pridelení kód (hash hodnota) a stávajú sa označenými dátami. Po označení sú dáta zabezpečené.

Balíček Externy informacny system

Balíček Externy informacny system predstavuje prácu navrhnutého systému s externým systémom. Komunikáciu riadi správca elektronickej komunikácie. Jeho úlohou je spravovať externý systém a informačný tok výkonu. V rámci externého systému je dôležité poznať funkcie systému. Na základe využitia externého systému pre navrhnutý systém, správca vytvára a edituje povolené funkcie systému.

Pre zvýšenie bezpečnosti elektronickej komunikácie je sledovaný aj tok výkonu. V prípade, že tok výkonu komunikácie je nižší (nestabilný), správca elektronickej komunikácie upravuje hranicu ochrany dát s cieľom zvýšenia bezpečnosti.

Balíček Monitorovanie udalosti

Navrhovaný systém je zameraný na bezpečnosť dát. Aby bola bezpečnosť udržateľná, bol vytvorený monitoring rizikových udalostí. Monitorované udalosti spravuje správca udalostí. V rámci systému monitorujeme osobné údaje klienta a identifikujeme úniky dát.

Osobné údaje používateľa sú zabezpečované. Pre popis zabezpečenia bola vytvorená procedúra Popis ochrany osobnych udajov. O určenie zabezpečenia sa stará správca utajovaných dát, ktorá určí, či tieto údaje sú citlivé, alebo sú verejné a priradí k nim príslušný spôsob šifrovania. Aby bol určený únik dát, bola vytvorená trieda Uniky dat. V rámci triedy zhromažďujem všetky úniky, ktoré nastali. Pri úniku je dôležitý popis, kde určím o aký únik ide, na aké dáta bol prevedený, akým používateľom a podobne.

Balíček Bezpecnostna politika

Každá operácia vykonávaná s dátami nesie riziká. Pre tieto riziká bola vytvorená trieda Rizika, ktorá vytvára popis rizika, kde boli určené rizikové procedúry s dátami. Pre riešenie rizikových procedúr bola vytvorená bezpečnostnú politiku pre riziko. Triedu Rizika spravuje manažér rizika. Jeho identifikačné číslo je priradené ku každému, ním vytvorenému, popisu, alebo bezpečnostnej politike.

Popis rizika ovplyvňuje aj správca utajovaných dát. Správca každému riziku priradí úroveň zabezpečenia. Na základe priradenia boli rozdelené riziká na úrovne zabezpečenia vzhľadom k dátam a operáciám. Určené riziká určujú hranicu ochrany. Hranica ochrany dát popisuje rámcové operácie, ktoré je možné prevádzať s dátami.

Odvodenie bezpečnostných pravidiel

Bezpečnostné pravidlá vychádzajú zo splnenia primárneho funkčného požiadavku na model, a to je uloženie dát do cloudu. Uloženie dát vyvolá koncový používateľ. Spracovanie tejto požiadavky znázorňuje sekvenčný diagram (Príloha E).

Dáta môže uložiť iba prihlásený koncový používateľ. Prihlásenie je opakujúca operácia s podmienkou kontroly prihlasovacích údajov. Po úspešnom prihlásení vyšle klient požiadavku na uloženie dát, ktorá je spracovaná na základe chronologického splnenia týchto bezpečnostných pravidiel (v zátvorke uvádzam aktéra z diagramu prípadu použitia, na ktorého sa toto pravidlo vzťahuje):

Pravidlo 1. Identifikovať vstupné dáta – na základe triedy Vstupne data systém určí aké dáta sa majú uložiť. *(manažér životného cyklu dát)*

Pravidlo 2. Požadovať zašifrovanie dát – po určení vstupných dát je potrebné požadovať zašifrovanie dát. *(koncový používateľ, adresár)*

Pravidlo 3. Zistiť úroveň zabezpečenia dát – každé dáta majú prisúdené povolené zabezpečenia dát vzhľadom k ich citlivosti. Na základe povolených zabezpečení je priradená úroveň zabezpečenia dát. *(manažér životného cyklu dát, súbor, správca utajovaných dát)*

Pravidlo 4. Nastaviť minimálne oprávnenia – minimálne oprávnenia sú rozšírením povolených zabezpečení dát. Minimálne oprávnenia určujú aké minimálne operácie sú povolené pre vykonávanie s dátami pričom operácie nespôsobia únik dát alebo nové riziká. *(manažér životného cyklu dát, súbor)*

Pravidlo 5. Zašifrovať dáta – na základe predchádzajúcich krokov 3 a 4 sú dáta zašifrované. *(manažér životného cyklu dát, adresár)*

Pravidlo 6. Označiť dáta – pre udržanie integrity dát je dátam prisúdený kód (hashovacia hodnota), označenie dát pozostáva z nasledujúcich krokov. *(manažér životného cyklu dát, manažér rizika, súbor)*

Pravidlo 7. Určiť riziká – pre označenie dát je potrebné určiť rizikové procedúry, ktoré môžu byť s dátami vykonávané a mohli by spôsobiť odcudzenie alebo úplnú stratu dát. *(manažér rizika, správca utajovaných dát)*

Pravidlo 8. Vytvoriť bezpečnostnú politiku – po určení rizík sa zostaví bezpečnostná politika, ktorá poukazuje na spôsob riešenia rizikových procedúr a spôsob ich predchádzania. *(manažér rizika)*

Pravidlo 9. Určiť hranicu ochrany – hranicu ochrany dát zostavíme na základe určených rizík a bezpečnostnej politiky. Definovaním hranice ochrany dát oddelíme rizikové operácie pre vykonávanie s dátami od bezpečných operácií. *(správca elektronickej komunikácie)*

Pravidlo 10. Zabezpečiť dáta – zabezpečené dáta sú zašifrované a majú priradený kód. Zabezpečené dáta obsahujú definované riziká, bezpečnostnú politiku a hranicu ochrany dát. *(adresár)*

Pravidlo 11. Vytvoriť typ zabezpečenia – zabezpečené dáta majú priradený typ zabezpečenia, teda zaradenie do bezpečnostnej úrovni v rámci úrovni dát nachádzajúcich sa v systéme. *(správca utajovaných dát, adresár)*

Pravidlo 12. Potvrdiť zabezpečenie – pokiaľ neobsahujú zabezpečené dáta typ zabezpečenia, nepovažujem dáta za zabezpečené. Po priradení typu systém vníma dáta za zabezpečené. *(manažér životného cyklu dát, správa utajovaných dát, správca udalostí)*

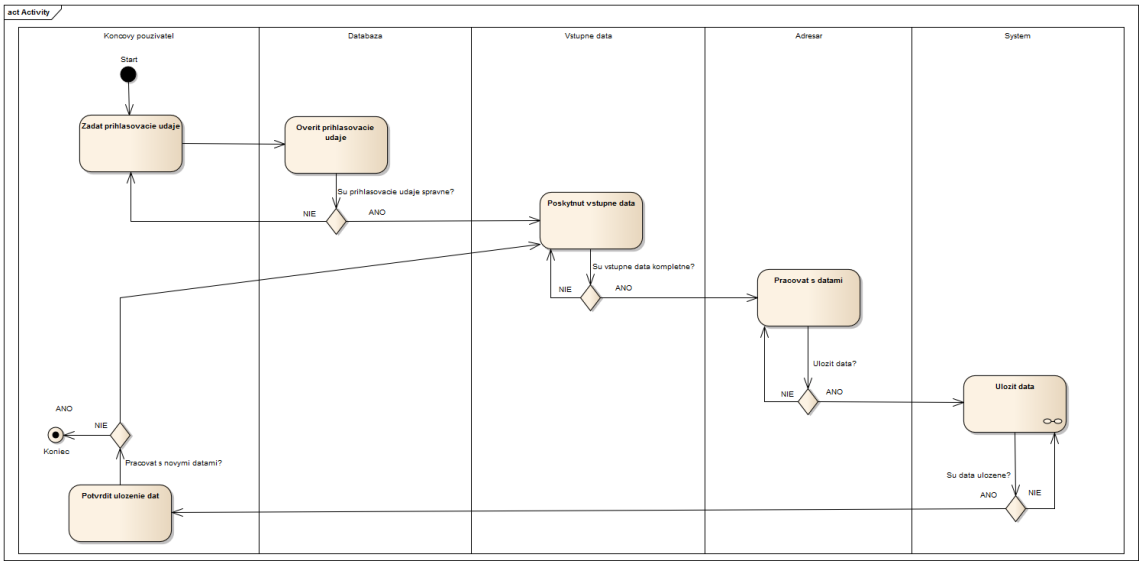
Pravidlo 13. Potvrdiť uloženie dát – po potvrdení správneho zabezpečenia dát, sú dáta uložené a koncový používateľ dostane informáciu o uložení dát. *(manažér životného cyklu dát, koncový používateľ, pamäťové médium, správca udalostí)*

Následnosť dodržiavania pravidiel 1 až 13 je striktne definovaná a výstup jedného kroku je vstupom pre druhý krok. Pravidlá nemôžu spracovávané paralelne. Pre tieto pravidlá vždy pracujú s operandom vstupné dáta. Pravidlá 3 a 4 sú pri vykonávaní typu slučky, ktorej podmienkou je určenie povolených zabezpečení. Pre správne vykonanie pravidla 4 je dôležité kontrolovať identifikačné číslo úrovne a minimálneho oprávnenia. Pri nekorektnosti údajov nastáva porušenie zabezpečenia dát v systéme. Pravidlá 7 až 11 predstavujú taktiež slučky, nakoľko bez ich správneho výstupu systém nesplní nasledujúce pravidlá 12 a 13.

Uvedené pravidlá sú naviazané k životnému cyklu ukladaných dát, ktorý popisujem v nasledujúcej podkapitole.

Životný cyklus ukladaných dát

Životný cyklus dát, ktoré chcem uložiť do cloudu prebieha v niekoľkých fázach. Podrobnejšiu špecifikáciu jednotlivých etáp a ich vzájomné vzťahy znázorňuje diagram aktivít (Obrázok 10). Diagram je tvorený z komunikácie medzi koncovým používateľom, databázou, vstupnými dátami, adresárom a systémom.



Obr. 10: Diagram aktivít životného cyklu

Diagram aktivít Uložiť dáta začína u koncového používateľa, ktorý zadáva prihlasovacie údaje. Tieto údaje sú kontrolované pomocou databázy, v ktorej sa nachádzajú prihlasovacie údaje klienta. Po úspešnom prihlásení sú klientovi poskytnuté vstupné dáta, s ktorými pracuje a následne ich chce uložiť.

Vstupné dáta sú poskytnuté z viacerých zdrojov (pamäťové médium, externý informačný systém a podobne), a preto je potrebné kontrolovať komplexnú dostupnosť

dát pre daného používateľa. Po kontrole je používateľovi umožnená práca s dátami, ktoré sú zatriedené do bezpečnostného adresáru. Následne po práci je umožnené uloženie dát do virtualizovaného prostredia. Táto aktivita je zložená z viacerých aktivít. Po finálnom ukončení všetkých jej aktivít je potvrdené uloženie dát zaslané klientovi a poskytnutá práca s ďalšími dátami bez kontroly prihlasovacích údajov.

V rámci aktivity Uložiť dáta spolu komunikujú zašifrované dáta, označené údaje, zabezpečené dáta a systém. Po úspešnom zašifrovaní dát je potrebné k dátam priradiť označenie a určiť riziká. Následne sú dáta zabezpečené s priradením typu zabezpečenia. Zabezpečené dáta sú ukladané na pamäťové médium, alebo do externého informačného systému. Obsah jednotlivých štrukturovaných aktivít je definovaný nasledovne.

Štrukturovaná aktivita Zašifrovať dáta (Príloha F)

Pre zašifrovanie dát je potrebné poznať povolené zabezpečenia dát, ktoré sú určené pre daný adresár. K povoleným zabezpečeniam dát je priradené úroveň zabezpečenia. Táto úroveň definuje rozdelenie dát z hľadiska citlivosti. Pokiaľ sú dáta vysoko citlivé, je potrebné nastaviť minimálne oprávnenia pre operácie vykonávané s dátami. Až po ich určení môžu byť dáta zašifrované.

Štrukturovaná aktivita Označiť dáta (Príloha G)

Skôr než dátam priradím jedinečný kód je potrebné určiť rizikové situácie, ktoré môžu nastať pri vykonávaní niektorých procedúr. Na základe rizík je určená bezpečnostná politika. Táto politika je obsahom hranice ochrany dát a na základe nej vytyčuje povolené operácie a zakázané operácie s dátami. Napokon sú vstupné dáta označené kódom.

Štrukturovaná aktivita Zabezpečiť dáta (Príloha H)

Označené dáta sú považované za zabezpečené na základe kontroly ich identifikátorov (rizikové procedúry, hranica ochrany dát a podobne). K zabezpečeným dátam je priradený typ zabezpečenia, čím považujem dáta za kompletne zabezpečené v rámci navrhovaného systému.

Sekvenčný diagram Uloženie dát

Sekvenčný diagram je naviazaný na prípad použitia Uloženie dát (Príloha E). Sekvencia začína od úvodnej správy od aktora Koncový používateľ. V rámci sekvenčného diagramu sledujem zasielanie správ medzi týmito prvkami: koncovy pouzivatel (aktor), klient, databaza, vstupne data, zasifrovane data, povolene zabezpecenia, adresar, urovne zabezpecenia, minimalne opravnenia, oznacene udaje, rizika, hranica ochrany, zabezpecene data (Priščáková a Rábová, 2013).

Pre uloženie dát je potrebné, aby bol koncový používateľ systému prihlásený. Z tohto dôvodu pred prácou s dátami požadujem prihlásenie. V rámci prihlásenia zasiela používateľ správu klientovi s požiadavkou na prihlásenie do systému. Klient je rozhranie, cez ktoré používateľ komunikuje zo systémom. Prihlasovacie údaje (meno a heslo) sú uložené v databáze, a preto Klient zasiela správu o požiadavke na overenie údajov triede Databáza. Po úspešnom overení údajov je používateľ prihlásený.

Nasledujúce správy postupujú za sebou chronologicky striktne a nie je ich možné vykonať skôr, prípadne upraviť ich pozíciu v rámci hierarchického rozpadu. Ulože-

nie dát spustí požiadavkou používateľ systému. Pokiaľ nebudú spracované všetky dáta, dovtedy budú vykonávané nasledujúce inštrukcie. Klient zistí vstupné dáta na základe triedy Vstupne data. Nasledne treba dáta zašifrovať, a teda trieda Vstupne data komunikuje s triedou Zasifrovane data. Pre zašifrovanie je potrebné určiť povolené zabezpečenia (povolené operácie) adresáru, v ktorom sa dáta nachádzajú. Tieto informácie sú uložené vo vlastnostiach každého adresára (trieda Adresar).

Po identifikovaní povolených zabezpečení je potrebné stanoviť úroveň zabezpečenia. To znamená, že trieda Povolene zabezpecenia zašle správu triede Urovne zabezpecenia. Ku každej úrovni zabezpečenia sú určené minimálne oprávnenia v triede Minimalne opravnenia. Minimálne oprávnenia slúžia pre určenie operácií, ktoré môžeme s dátami vykonať. Tieto oprávnenia môžu byť zmenené na základe zmeny prisúdenej úrovni zabezpečenia. Určením uvedených operandov sa pristúpi k zašifrovaniu dát. Týmto je splnený prvý krok zabezpečenia dát.

Druhým krokom je označenie dát, teda priradenie hodnoty k dátam. Pre označené dáta máme triedu Oznacene udaje. Skôr než je dátam priradená hodnota, je potrebné identifikovať riziká. V triede Rizika sú zaznamenané všetky rizikové procedúry a operácie, ktoré s dátami môžu byť prevedené. Na základe ich identifikácie sa vytvorí bezpečnostná politika, ktorá tvorí plán eliminácie dopadov vzniknutých rizík.

Na základe určenia rizík a bezpečnostnej politiky sa k dátam priradí hranica ochrany dát, teda stupeň ich citlivosti. Vďaka hranice ochrany zadefinujeme operácie, ktoré sú pre prácu s dátami prípustné.

Až po uložení hranice ochrany je k dátam priradený kód (hashovacia hodnota). Takéto dáta sú už zabezpečené, keďže splnili navrhovanú metodiku a môžu byť uložené do dátového úložiska. Posledná správa je informatívneho charakteru a oznamuje koncovému používateľovi, že dáta boli uložené.

3.2 Formalizácia navrhnutej metodiky

Pri stanovení metodiky implementácie cloud computingu v podnikovom a univerzitnom prostredí boli použité dva základné prístup, a to pohľad z hľadiska konečných automatov a pohľad z hľadiska Petriho sietí.

Prvý pohľad predstavuje realizáciu formalizácie na základe stanoveného životného cyklu dát s ohľadom na zvýšenie bezpečnosti dát uložených v cloude. Definovaný životný cyklus predstavuje nedeterministický konečný automat. Nedeterministickosť automatu vyplýva z možnosti odcudzenia dát. Konečnosť automatu predstavuje stav uloženia dát do cloudu. Pre vytvorenie tohto automatu bola využitá metóda určenia bezpečnostných aspektov pre navrhovaný model. Výsledky prístupu z pohľadu konečných automatov definovali bezpečnostné pravidlá.

Pohľad na metodiku z hľadiska Petriho sietí zhrnul stanovené pravidilá a ich aplikáciu do životného cyklu spracovávania požiadavky na uloženie dát do cloudu. Hlavnou výhodou Petriho siete je simulácia, ktorá poukázala na možné riziká navrhovanej metodiky. Prístup k Petriho sieti je rozdelený do dvoch podčastí, a to

z pohľadu grafického a z pohľadu matematického vyjadrenia. Stanovené matematické vyjadrenia definovali navrhovaný model a bezpečnosť dát pre zovšeobecnenie do podoby formalizácie metodiky.

Determinovanie bezpečnostných aspektov

V prípade požiadavky zvýšenia bezpečnosti dát, je potrebné v navrhnutom modeli určiť bezpečnostné aspekty, ktoré ovplyvňujú celý model. Pre dosiahnutie zovšeobecného využitia navrhovaného modelu boli určené tieto pravidlá:

- prihlásenie používateľa,
- šifrovanie a bezpečnosť dát,
- riziká,
- integrita dát.

Pravidlá v sebe zahŕňajú odvodené bezpečnostné pravidlá a stali sa vstupom pre určenie oblastí v nedeterministickom konečnom automate a Petriho siete.

Pravidlá pre prihlásenie používateľa

Pravidlo 1. Vložiť prihlásenie pomocou formulára.

Pravidlo 2. Dáta je potrebné overovať prostredníctvom databázy; databáza je umiestnená na serveri.

Pravidlo 3. Po úspešnom overení, je udelený prístup k systému a vstupným dátam; vstupné údaje sú závislé na prihlásení.

Pravidlo 4. Vstupné dáta sú overované v časovýc intervaloch; pokiaľ nie je dovolené vstúpiť do dát, je odoslaná požiadavka na opätovné prihlásenie.

Pravidlo 5. Po dokončení práce s dátami koncový používateľ zadá požiadavky na ukladanie dát.

Pravidlá pre šifrovanie a bezpečnosť dát

Pravidlo 1. Dáta sú zaradené do kategórií citlivosti (verejné, citlivý, tajné); každá kategória má inú istotu.

Pravidlo 2. Úroveň zabezpečenia má minimálne oprávnenie; minimálne oprávnenia sú oprávnenia pre koncového používateľa pre jeho prácu s dátami.

Pravidlo 3. Ak sú minimálne oprávnenia nedostačujúce, je potrebné stanoviť nové oprávnenia; nové oprávnenia sú priradené k súboru dát.

Pravidlo 4. Systém vyžaduje šifrovanie po zistení povolenia.

Pravidlá pre riziká

Pravidlo 1. Riziká sú určené po šifrovaní dát; riziká sú postupy, ktoré spôsobujú odcudzenie dát; databáza ukladá riziká, ktoré boli doteraz identifikované; ak sa určí nové riziko, je vložené do databázy; v prípade, že riziko je už v databáze, je zmenené, pokiaľ ide o proces spracovávania dát.

Pravidlo 2. Bezpečnostná politika je založená na zistených rizikách; bezpečnostná politika je postup ako sa vysporiadať s rizikom, ktoré je zaznamenané v databáze.

Pravidlo 3. Bezpečnostná politika je určená hranicou ochrany údajov; hranica ochrany údajov určuje vhodné a nevhodné postupy pre dáta; hranicu ochrany dát možno meniť len v prípade, že databáza je lokálna.

Pravidlá pre integritu dát

Pravidlo 1. Dáta sú identifikované priradením konkrétneho typu hodnoty v prípade externého pamäťového média.

Pravidlo 2. Pre zaistenie dát je priradená k údajom hashovacia hodnota.

Pravidlo 3. Pre dodržanie integrity dát určím typ zabezpečenia viažúci sa k dátam; typ zabezpečenia je stupeň, spôsob a algoritmus zabezpečenia dát; táto hodnota má vplyv na hranicu ochrany dát, bezpečnostnú politiku, riziko a minimálne oprávnenia.

Pravidlo 4. Dáta sú uložené po splnení predchádzajúcich pravidiel.

Pravidlo 5. V prípade, že koncový používateľ požaduje pokračovanie po uložení dát, je potrebné zabezpečiť vstup.

Formalizácia metodiky prostredníctvom Petriho siete

Pre overenie a formalizovanie navrhnutého modelu zvýšenia bezpečnosti ukladania dát do cloudu sa transformoval diagram aktivít do prostredia Petriho siete (Príloha I). Pri simulácii prevedeného diagramu aktivít bolo identifikovaných 14 kolíznych situácií v prechodoch: potreba overenia, sprava overenia, sprava overenia dat, praca s datami, pozadovat ulozenie dat, potreba povolenych zabezpeceni, zmena opravneni, overit minimalne opravnenia, pozadovat zasifrovanie dat, sprava o urcenych rizikach, pozadovat hranicu ochrany, sprava oznacenia, sprava o ulozeni, poskytnut vstup.

Uvedené kolízie spôsobili ukončenie simulácie po dvoch cykloch. Riešenie kolíznych situácii sa zabezpečilo presmerovaním toku tokenu, pridaním nových miest a pridaním vstupných tokenov v miestach Server – Subor, Rizika, Hranice ochrany dat.

Pre identifikáciu možných ukončení simulácie boli vložené miesta Neuspesne zasifrovanie, Data neoznacene, Neuspesne zabezpecene, Ukoncit. Uvedené miesta predstavujú stavy, v ktorých môže byť model ukončený. V prípade miesta Ukoncit ide o fyzické ukončenie práce s aplikáciou na vyžiadanie koncového používateľa. Miesta Neuspesne zasifrovanie, Data neoznacene, Neuspesne zabezpecene reprezentujú negatívne stavy, v ktorých simulácia skončí v prípade neúspešného vykonania predchádzajúceho procesu. Tieto negatívne stavy je možné vyriešiť tak, aby ich stav bol prepojený so stavom opätovného navrátenia do systému.

Petriho sieť je rozčlenená do 4 hlavných blokov zodpovedajúcich pravidlám uvedených v determinovaní bezpečnostných pravidiel. *Prvý blok (červený)* predstavuje riešenie od prihlásenia používateľa cez jeho overenie až po sprístupnenie patričných údajov. *Druhý blok (modrý)* simuluje procesy overenia povolených zabezpečení, definovanie úrovne zabezpečenia na základe používateľa, kontrolu minimálnych oprávnení (prípadne ich nastavenie) až po požiadavku pre zašifrovanie dát. *Tretí blok (zelený)* charakterizuje prácu s rizikami, pričom najprv riziká definuje a vykoná s nimi

potrebné operácie, a až tak následne určí hranicu ochrany dát. *Štvrtý blok (žltý)* je určený pre integritu dát. V rámci tohto bloku môže systém skončiť v dvoch negatívnych stavoch, a to buď dáta neboli správne označené, alebo správne neprebehla operácia so zabezpečením.

Ďalšie miesta a prechody, ktoré sa v Petriho sieti nachádzajú, sú určené pre spracovanie uloženia dát a opätovné pokračovanie koncového používateľa v práci so systémom.

Simulácia a analýza Petriho siete

Pred simuláciou Petriho siete bola nastavená hodnota kroku na 1 ms, čas pre ukončenie simulácie na 1 000 ms a maximálny počet krokov simulácie na 1 000. Petriho sieť pozostáva z 22 prechodov a 33 miest. Hodnota váhy hrany je vo všetkých prípadoch 1 (C/T Petriho sieť). Kapacita miest je prevažne 1, iba miesta, ktoré slúžia ako koncové stavy modelu majú kapacitu určenú na hodnotu 100. Prechody sú zadefinované bez čakania s časovým modelom okamžitým.

Pri prvej analýze simulácii bolo využité krokovanie, aby bolo možné vidieť správanie sa jednotlivých prechodov a miest. Správanie sa jednotlivých miest a prechodov počas každého kroku neuvádzam v práci z dôvodu rozsahu analýzy.

V Petriho sieti platí definícia:

Označme p(t) počet tokenov v mieste p. Potom pre každý prechod platí, že $p(t)_i > 0$ *pre všetky vstupné miesta* p_i *tohto prechodu.*

Z tejto definície vyplýva charakteristika navrhnutých prechodov. Uvedené definície sú matematicky vyjadrené na základe blokov Petriho siete, ich miest, prechodov a správania sa tokenov.

Pre matematické vyjadrenie platí, že a je množina vstupných dát konkrétneho koncového používateľa, A je množina všetkých dát, b je konkrétna usporiadaná dvojica údajov meno a heslo pre prihlásenie používateľa, B je množina všetkých usporiadaných dvojíc prihlasovacích údajov používateľov, c reprezentuje dáta konkrétneho používateľského účtu, C je množina všetkých dát viažúcich sa k používateľským účtom, d je konkrétna úroveň zabezpečenia, D je množina všetkých dostupných úrovní zabezpečenia, E je množina všetkých povolených zabezpečení, pričom je tvorená usporiadanou dvojicou d a e, kde e je konkrétne zabezpečenie, f sú všetky dostupné minimálne oprávnenia (aj aktualizované), g je množina konkrétny šifrovaných dát, G je množina všetkých šifrovaných dát, h je konkrétna množina údajov o hranici ochrany dát, i je množina údajov o bezpečnostnej politike, j je množina kokrétny údajov o rizikách, J je množina všetkých dostupných rizík.

Definícia 1. Poskytnutie vstupných dát koncovému používateľovi môže nastať iba vtedy, ak správa overenia prihlási používateľa do systému a priradí dáta k používateľskému účtu.

Matematické vyjadrenie 1.

b$\cap c \neq \oslash \Rightarrow \exists c \in C$, pre ktoré platí $c \equiv a$, pričom $a \subseteq A$, potom sú dáta sprístupnené. (2)

Definícia 2. Ak systém chce určiť úroveň zabezpečenia používateľa, potom musí sprístupniť súbor povolených zabezpečení nachádzajúci sa na servery a vykonať verifikáciu povolených zabezpečení.

Matematické vyjadrenie 2.

$\exists e \in E$ pre ktoré platí, že $[d, e] \equiv [c, a]$, pričom $[d, e] \subset Ea[c, a] \subset c \cap e$, potom $d \equiv [c, a]$. (3)

Definícia 3. Pre zašifrovanie dát je potrebné načítať minimálne oprávnenia a zmeny prevedené v minimálnych oprávneniach.

Matematické vyjadrenie 3.

$\exists f, \Delta f$ pre ktoré platí, že $f \cap e = c$, potom $g = a$ pričom $g \subset f \subset e \subset c$. (4)

Definícia 4. Určené riziká sú zostavené na základe doposiaľ určených rizík uložených v systéme a nových identifikovaných rizikových procedúr, pričom nová riziková operácia nemôže byť už uložená v systéme.

Matematické vyjadrenie 4.

j=$\Delta j \cup j$, pričom $j \in J$. (5)

Definícia 5. Pre pridelenie hranice ochrany je potrebné načítať doposiaľ určenú hranicu ochrany dát a vytvorenú bezpečnostnú politiku pre tento typ dát.

Matematické vyjadrenie 5.

h=$\Delta h \cap i$, pričom $h \subset d \vee i \subset E$, kde $i \equiv e \cup i \equiv j$. (6)

Definícia 6. Ak je poskytnutý opätovný vstup do systému, potom dáta neboli uložené alebo dáta nie sú povolené k používateľovmu účtu, alebo klient potvrdil pokračovanie v práci.

Matematické vyjadrenie 6.

a=$\oslash$ pričom $(a \cup c) \neq g \wedge a \neq c$, potom $c \equiv b$. (7)

Výsledná definícia Petriho siete modelu zvýšenia bezpečnosti dát ukladaných do cloudu, ktorá zhrňuje uvedených 6 definícií z pohľadu komplexnosti je nasledujúca:

Petriho sieť modelu zvýšenia bezpečnosti dát ukladaných do cloudu je bezpečná, ohraničená a konzervatívna, pretože pre každé jej ohodnotenie platí $z(p) \leq 1$, pričom $\exists k \in N_0; \forall z, p; z(p) \leq k$.

Nedeterministický konečný automat

Pre podporu verifikácie rámcovej metodiky som zostavila nedeterministický konečný automat (Príloha J). Tento automat vyplýva z Petriho siete, bezpečnostných pravidiel a navrhnutej metodiky, pričom výstupom automatu sú pravidlá bezpečnosti dát v cloude pre automat.

Nedeterministický konečný automat je špecifikovaný ako $A = (K, , , q0, F)$, kde
$K = \{q0, q1, q2, \ldots, q32\}$,
Σ=a, b, c, d, x, z,

kde a je prihlasovací údaj, b sú nezabezpečené dáta, c je integrita dát, d sú uložené dáta, x je zlyhanie systému, z je ukončenie práce.

Nastavenie počiatočného stavu je nasledovné $q0 = (q0)$.

Konečná množina stavov je nasledujúca $F = \{q0, q16, q25, q27, q32\}$,

kde q0 je vstupný používateľský údaj, q16 je neúspešné šifrovanie, q25 je nezaradenie dát, q27 je neúspešnosť zabezpečenia, q23 je kompletné spracovanie, ukončenie práce.

Pre príklad uvádzam správne vstupné slovo: abbbbbbbbbbbbbccccda.

Z automatu vyplývajú pravidlá, ktorými sa riadi:

Pravidlo 1. Správne vstupné slovo musí obsahovať písmená a, b, c, d.

Pravidlo 2. Vstupné slovo má obsahovať reťazec bcccc pre zachovanie integrity dát.

Pravidlo 3. Vstupné slovo pre akceptovanie automatom spĺňajúce bezpečnostné podmienky začína na písmeno a a končí na písmeno a. Takýto reťazec ukladá dáta a pokračuje v práci.

Pravidlo 4. V prípade, že vstupné slovo obsahuje reťazec cx na konci slova, potom integrita dát je splnená, avšak dáta nie sú uložené.

Pravidlo 5. Ak vstupné slovo má písmeno x na konci vstupného slova, potom vstupné slovo je nesprávne. Automat je ukončený pred splnením bezpečnostných podmienok.

Pravidlo 6. V prípade, že vstupné slovo obsahuje písmeno z na konci slova, potvrdzuje to správnosť slova. Dáta sú zabezpečené a koncový používateľ ukončil prácu.

Pravidlo 7. Ak vstupné slovo obsahuje reťazec xx na konci slova, tak to znamená, že údaje nie sú k dispozícii pre vstup prihláseného používateľa.

Metodika implementácie

Na základe uvedených návrhov vyvodených z teoretických východísk bola zostavená metodika implementácie cloud computingu pre podnikové a univerzitné prostredie. Základom metodiky bolo zvýšiť bezpečnosť dát, ktoré sú ukladané do cloudu. Navrhnutá metodika je vhodná pre obe uvedené prostredia a pozostáva z 15 krokov. Uvedené kroky vyplývajú z doposiaľ stanovených predpokladaných pravidiel a definícií. Odlišnosti v jednotlivých krokoch sú uvedené rozdelením kroku na časť a (podnikové prostredie) a časť b (univerzitné prostredie). Súhrn rozdielov je uvedený vo verifikácii metodiky.

Krok 1. Analyzovať implementačné prostredie a identifikovať dostupný hardvér.

Pred samotnou implementáciou je potrebné previesť hĺbkovú analýzu prostredia. Okrem rozdelenia prostredia (podnikové alebo univerzinté) je potrebné jasne definovať využitie cloudu a požiadavky koncových používateľov. Analýza zahŕňa aj identifikáciu hardvéru, ktorý aktuálne disponuje podnik, alebo univerzita. Pokiaľ je hardvér nedostačujúci, odporúčam využiť návrh infraštruktúry, ktorý je v práci uvedený. Implementáciu cloud computingu ovplyvňujú aj hardvérové možnosti, pričom je potrebné porozumieť vzťahu medzi požiadavkami, využitím a hardvérom.

Krok 2. Stanoviť aktérov pre implementáciu a následnú prevádzku systému.

Na základe využitia cloud computingu a analyzovania požiadaviek koncových používateľov sa stanovia aktéri, ktorí budú so systémom pracovať. Každý aktér bude v kroku 13 zaradený do autorizačnej úrovne.

Krok 2a. V podnikovom prostredí je potrebné identifikovať týchto aktérov: klient firmy, koncový používateľ, manažment firmy, pracovník IT oddelenia.

Krok 2b. V univerzitnom prostredí je potrebné identifikovať týchto aktérov: zainteresovaná osoba, študent (interný aj externý), akademický pracovník (interný aj externý), manažment univerzity, pracovník IT oddelenia.

Krok 3. Identifikovať zdroje dát.

V navrhovanom modeli pracujem s viacerými typmi zdrojov dát. Základná identifikácia zdrojov by mala byť rozdelená na pôvod typu interný/externý zdroj (fyzický disk), interný/externý zdroj (cloud), externý harddisk, CD/DVD, flash disk, mobilný počítač, mobilný telefón. Dáta vložené zo zdroja by mali so sebou niesť informáciu o pôvode a oprávneniach.

Krok 4. Priradiť aktérom oprávnenia pri práci s dátami.

Každému aktérovi je potrebné priradiť oprávnenia, ktoré zahŕňajú možné operácie prevádzané s dátami. Oprávenia sú ovplyvnené požiadavkami koncových používateľov a zaradením do skupiny aktéra.

Krok 4a. V podnikovom prostredí aktéri majú tieto oprávnenia:

- klient firmy a jeho oprávnenia sú zavislé na type a zameraní firmy; v prípade, že firma pracuje na základe zakázky, ktorá je vkladaná cez informačný systém, klient firmy by mal zadávať dáta potrebné pre vytvorenie zakázky s možnou podporou jej kalkulácie a vytvorenia predbežnej faktúry; pokiaľ firma potrebuje

zabezpečiť klientovi možnosť nie len vkladania, ale aj editácie a vyhľadávania vnútorných informácií o firme, je potrebné zvýšiť bezpečnosť dát a klientovi poskytnúť iba nutné informácie o podniku; oprávnenia nie je možné definovať na základe veľkosti firmy a jej klientov,

- koncový používateľ je zamestnanec firmy, ktorý pracuje s citlivými údajmi (vnútorné a dôverné dáta); koncovému používateľovi sú pripradené operácie vloženie, editovanie, mazanie, vyhľadávanie s dátami, ktoré sú naviazané na jeho autorizačný stupeň a jeho požiadavky práce (zaradenie zamestnanca na pozíciu a oddelenie); v prípade malých firiem je často koncový používateľ aj manažmentom firmy,
- manažment firmy má priradené všetky možné operácie vykonávania s dátami, pričom má zákaz úpravy systému,
- pracovník IT oddelenia má prednostne priradené oprávnenia pre správu systému, pričom môže na dáta nahliadnuť z pohľadu všetkých aktérov a vykonávať príslušné operácie; v prípade malej firmy je pravdepodobné, že tento aktér vo firme nie je, a preto sa ním stáva tretia strana (poskytovateľ cloudu.

Krok 4b. V univerzitnom prostredí aktéri majú tieto oprávnenia:

- zainteresovaná osoba je osoba, ktorá sa zaujíma o chod univerzity, alebo je s univerzitou spojená z dôvodu dodávateľskej zmluvy, prípadne ide o osobu, ktorá je s univerzitou zviazaná počas stanoveného časového obdobia (konferencie, prednáška); z toho vyplýva, že oprávnenia osoby vznikajú na základe jej prepojenia s univerzitou; v prípade, že sa jedná o potencionálneho študenta, tak je vhodné oprávnenia nastaviť na vkladanie a editáciu dát potrebných s prijímacou skúškou; pokiaľ je osoba účastník konferencie, je vhodné oprávnenia definovať tak, aby mu boli poskytnuté aj vnútorné údaje, ktoré súvisia s konferenciou a zadelenou sekciou; v prípade dodávateľa sú oprávnenia naviazané výlučne na operácie vkladania a úpravy dát plynúcich z naplnenia dodávateľskej zmluvy,
- študent (interný aj externý) čiastočne pracuje s vnútornými dátami, a preto jeho operácie sú obmedzené; oprávnenia študentovli povoľujú manipulovať a vykonávať základné operácie s dátami, avšak iba v nižšej úrovni, kde nie sú zahrnuté citlivejšie údaje; taktiež údaje, ktoré sú považované za dôvernejšie sa buď nezobrazujú, alebo pokiaľ je nutné ich zobrazenie, neumožňujú editáciu a samotné vkladanie tohto typu údajov,
- akademický pracovník (interný aj externý) pracuje s citlivejšími údajmi ako študent, avšak jeho oprávnenia čiastočne poskytujú aj reporty s dátami; povolené operácie s dátami sú zavislé vzhľadom k jeho zaradeniu,
- manažment univerzity môže vykonávať všetky druhy operácií spojených s dátami všetkých typov; jediné obmedzenie spočíva v úprave dát spojených so správou implementovaného systému,

- pracovník IT oddelenia má rovnaké oprávnenia ako v podnikovom prostredí, pričom je dôležité poznamenať, že tento pracovník môže byť aj akademickým pracovníkom; v univerzitnom prostredí sa nepredpokladá tretia strana v prípade, že sa nejedná o detašované pracovisko, prípadne univerzitu s nízkym počtom akademických pracovníkov a študentov.

Krok 5. Definovať požadované operácie z hľadiska bezpečnosti dát.

Po identifikovaní požiadaviek a z nich plynúcich operácií je potrebné bezpečnostné zaradenie. Každá operácia s dátami je analyzovaná a zaradená do súboru s minimálnymi oprávneniami a oddeleniami povinností. Tieto súbory sú následne prepojené s aktérmi.

Krok 6. Určiť rizikové procedúry.

Všetky súbory obsahujúce zaradenie operácií sú analyzované z pohľadu definovania rizík. Procedúry, ktoré by mohli ohroziť spoločnosť alebo univerzitu z pohľadu odcudzenia dát sú odpamätávané. K rizikovým procedúram sú radené procedúry, ktoré v sebe zahrňujú vymazávanie, zmenu citlivých dát a prípadne ukladanie na externý zdroj.

Krok 7. Definovať hranicu ochrany pre jednotlivých aktérov.

Hranica ochrany slúži pre obmedzenie oprávnení jednotlivých používateľov systému. Priradená hranica ovplyvňuje rizikovú politiku, nakoľko jej určuje možné operácie. Hranica ochrany pre jednotlivých aktérov vyplýva z kroku 3.

Krok 8. Determinovať kroky rizikovej politiky.

Podnikové aj univerzitné prostredie by malo mať stanovenú rizikovú politiku. Determinovanie jednotlivých krokov je vždy prepojené s konkrétnou rizikovou procedúrou. Nakoľko rizikové procedúry si môžu byť podobné, avšak nie totožné, niektoré kroky rizikovej politiky sú zhodné. Cieľom rizikovej politiky je určiť postup vykonania operácií. Vykonanie krokov rizikovej politiky minimalizuje dopad rizík, ktoré nastali prevedením príslušných operácií.

Krok 9. Konfigurovať primárny server pre dátové úložisko.

Po prevedenej analýze a stanovení výsledkov jednotlivých krokov je potrebné prejsť ku konkrétnej implementácii. Úvodná konfigurácia servera je založená na určení rozdelenia diskových polí (RAID-Z) (Priščáková, 2014), použitom súborovom systéme, výberu šifrovacieho systému.

Krok 10. Implementovať virtualizačnú technológiu a zvolený operačný systém.

Na základnú konfiguráciu servera je implementovaná virtualizačná technológia. V tomto kroku je potrebné nastaviť jej konfiguráciu. Pre kompletnú implementáciu je potrebné zahrnúť aj operačný systém.

Krok 11. Klonovať konfiguráciu na sekundárny server.

Nastavenie primárneho serveru je klonované na sekundárny server z dôvodu totožnej konfigurácie serverov.

Krok 12. Aplikovať navrhnutú infraštruktúru siete.

Dátové úložisko je prepojené na základe navrhnutej infraštruktúry siete.

Krok 13. Vytvoriť prihlasovacie účty pre koncových používateľov.

Prihlasovacie účty sú vytvorené na základe autorizačných úrovní, koncovým používateľom sú priradené kľúče a definované oprávnenia.

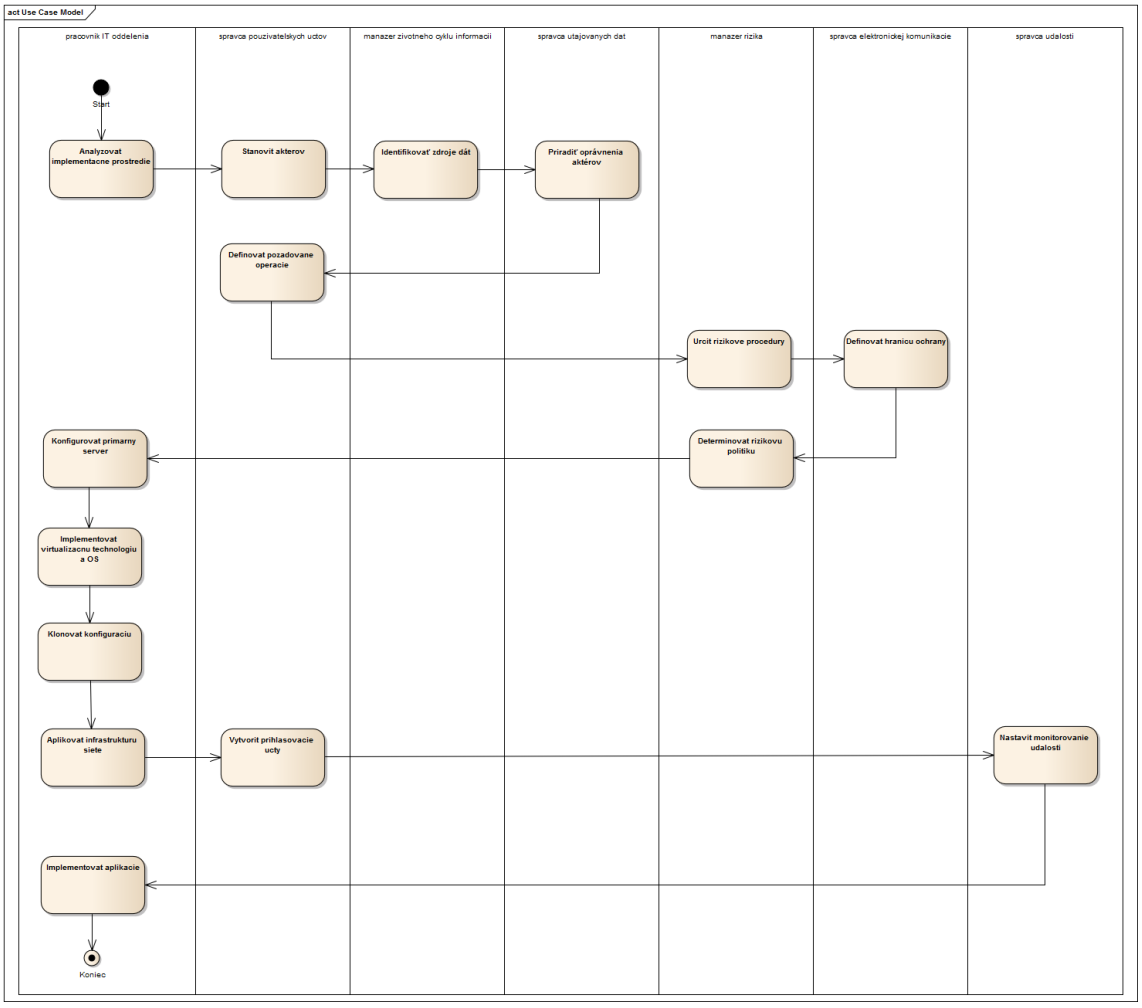
Krok 14. Nastaviť monitorovanie udalostí.

Pomocou manažéra v navrhnutej infraštruktúre nastaviť monitorovanie udalostí.

Krok 15. Implementovať potrebné aplikácie na aplikačný server.

Posledným krokom je implementácia samotných aplikácií, ktoré koncoví používatelia potrebujú.

Uvedené kroky metodiky sú zovšeobecnené a obsahujú odkazy na návrh architektúry a infraštruktúry, ktoré uvádzam pri verifikácii navrhnutej metodiky. Vzťah medzi jednotlivými krokmi metodiky a aktérmi uvedenými v navrhnutom modeli zabezpečenia dát ukladaných do cloudu v use case diagrame uvádzam v diagrame aktivít na obrázku 11.



Obr. 11: Diagram aktivít navrhnutej metodiky

3.3 Verifikácia navrhnutej metodiky

Navrhnutý model zvýšenia bezpečnosti dát ukladaných v cloude a stanovená metodika bola overená v prostredí stredného podniku a univerzity. Stanovené kroky metodiky sú verifikované prostredníctvom:

- *hrubého návrhu architektúry*, ktorý predstavuje stanovenie jednotlivých celkov architektúry typu klient-server so zameraním na ukladanie a zabezpečenie dát a komunikácie medzi klientom a serverom počas využívania cloudovej aplikácie,
- *návrhu infraštruktúry*, ktorá je najprv všeobecne charakterizovaný schémou infraštruktúry, pričom je zameraný na bezpečnosť dát z pohľadu hardvéru a softvéru, ako aj minimálne náklady na vytvorenie dátového centra,
- *implementáciu a testovanie technológií*, čo predstavuje súhrn použitých softvérových produktov, ktoré boli využité pre zvýšenie bezpečnosti s ohľadom na stanovenú architektúru a infraštruktúru. Zároveň táto etapa obsahuje výsledky testovania nasadených technológií a načrtnutie zrhnutia výskumu.

Uvedené činnosti verifikácie zahrňujú stanovené bezpečnostné pravidlá. V závere podkapitoly je uvedené finálne zrhnutie vykonanej verifikácie metodiky.

Hrubý návrh architektúry

Architektúra je základom pre metodiku a jej implementáciu. Výskum tejto práce je zameraný na ukladanie dát v cloud computingu z pohľadu používateľa a jeho požiadaviek. Z tohto dôvodu vyplýva aj typ zaradenia architektúry, a teda klient-server. Pre dosiahnutie globálnejšieho pohľadu na architektúru nie je umožnené pristupovať k blokom architektúry detailnejšie, a preto sú stanovené z hľadiska všeobecne využiteľných možností.

Na základe uvedených teoretických východísk práce sú stanovené tieto základné bloky architektúry (Priščáková a Rábová, 2014):

- dáta,
- klasifikácia dát,
- redundancia dát,
- správa kľúčov,
- autorizačné úrovne,
- šifrovací systém,
- TLS,
- HTTPS,
- nastavenie latencie.

Dáta

Základom architektúry sú dáta. Ide o údaje, ktoré vložil koncový používateľ zo strany klienta cez prehliadač. V tomto prvom bloku architektúry je bližšie charakterizovaná identifikácia dát, teda ich pôvod, typ, klasifikáciu a podobne. Je to z toho dôvodu, že zo strany koncového používateľa nie je vhodné, aby tieto informácie poskytoval, respektíve jedinou úlohou koncového používateľa je vložiť údaje bez znalostí o ich detailnej špecifikácii.

Navrhnutá architektúra podporuje 3 spôsoby vloženia dát, a to priame vkladanie koncovým používateľom, vloženie z externého média a prepojenie z externého informačného systému. Z pohľadu bezpečnosti vkladaných dát predstavujú všetky spôsoby riziko odcudzenia dát.

V podnikovom prostredí predstavuje vkladanie dát uvedené riziká. V prípade koncového používateľa ide o možnosť zverejnenia tretím stranám. Vloženie z externého média je považované za bezpečné pokiaľ prebieha kontrola pinov. Prepojenie s externým informačným systémom predstavuje riziko pri komunikácii medzi systémami, ktorá je zabezpečená, avšak môže dôjsť k jej odpočúvaniu.

V univerzitnom prostredí riziko koncového používateľa je zhodné s podnikovým prostredím. V rámci vloženia dát z externého média je kontrola pinov možná iba v prípade, že koncový používateľ využíva pripojenie priamo cez univerzitnú sieť. Z toho vyplýva, že bezpečnosť vkladaných dát z globálnej siete Internet predstavuje reálnu hrozbu. Pre vloženie dát z externého informačného systému platí rovnaké riziko ako pri podnikovom prostredí.

Klasifikácia dát

Vložené dáta je potrebné klasifikovať. Priradením klasifikačného stupňa dáta roztriedime podľa citlivosti. V navrhnutej architektúre bola využitá klasifikácia podľa Winklera (Winkler, 2011).

V podnikovom prostredí sú využité 4 klasifikačné stupne dát. Verejné dáta prestavujú najnižšiu úroveň, ktorá nie je zabezpečená z pohľadu navrhnutej metodiky, nakoľko je dostupná v rámci globálnej siete Internet. Medzi tieto dáta radím všeobecnú charakteristiku firmy. Dáta pre vnútorné použitie predstavujú prvý zabezpečený stupeň. Pôvodcom dát je buď manažment, ktorý informácie rozposiela v rámci podniku, alebo externý informačný systém, ktorý je zabezpečený. Tretím klasifikačným stupňom sú dáta dôverné, a teda dáta konkrétneho koncového používateľa. Štvrtým, a zároveň najvyšším stupňom bezpečnosti sú dáta tajné. Do tohto stupňa radím reporty, nasadené osvedčené postupy a podobne. (Priščáková a Salák, 2014)

V univerzitnom prostredí sa menia klasifikačné stupne z dôvodu typu dát a použitého prostredia. Najnižšia úroveň verejných dát ostáva nezmenená. Ide o všeobecné informácie o univerzite, ktoré sú voľne dostupné. Druhá úroveň je zabezpečená, keďže do tohto stupňa radím údaje v rámci vnútorného informačného systému univerzity. Pôvodcom údajov sú akademickí pracovníci, manažment univerzity, študenti, externí pracovníci, administrátori a podobne. Tretiu úroveň zahŕňajú dáta vytvorené a určené pre manažment univerzity. Z definovania týchto stupňov vyplýva, že pô-

vodný tretí klasifikačný stupeň v podniku je na univerzite nevyužitý, nakoľko údaje druhého klasifikačného stupňa v univerzitnom prostredí sú dostupné napríklad administrátorom, a teda udržanie dôvernosti dát jednotlivca v rámci univerzitného informačného systému je bezpredmetné.

Redundancia dát

Z pohľadu bezpečnosti dát a udržania integrity dát je nutné ukladať dáta redundante. Z toho dôvodu sa v tejto architektúre pracuje výlučne s redundantnými dátami. Detailnejšia redundanciu dát je v návrhu infraštruktúry.

Z hľadiska podnikového a univerzitného prostredia je dôležité dodržiavať redundanciu dát. Rozdiel v jej riešení spočíva vo využití hardvéru a softvéru. Ďalším možným rozdielom je využitie služieb poskytovateľa cloudu, pričom táto možnosť je viac využiteľná pre testovaný stredný podnik, než pre univerzitu vzhľadom k technickým možnostiam a počtu koncových používateľov.

Správa kľúčov

Správa kľúčov úzko súvisí s autorizačnými úrovňami. Platí všeobecné tvrdenie, že správa kľúčov je rovnako dôležitá pre podnikové a univerzitné prostredie. Každý koncoví používateľ má priradený kľúč, na základe ktorého pracuje v informačnom systéme s dátami. Základom pri komunikácii je stanovenie kľúču relácie a univerzálneho kľúču. Kľúč relácie slúži pre správu komunikácie v rámci daného sedenia. Univerzálny kľúč je využitý pre overenie identity druhej strany, a zároveň priradenie kľúču relácie. Pre minimálne zabezpečenie je nutné časovo zabezpečiť univerzálne kľúče pomocou časového razítka (definovaný čas do expirácie). V prípade, že v sedení vystupuje tretia strana napríklad ako distrubučné centrum kľúčov, je potrebné dodržanie dôvery.

Pre každý kľúč platí hierarchia miest s kľúčmi, pričom sa preferuje lokálne nastavenie. V rámci správy kľúčov je nutné každému kľúču definovať povolené použitie. Pri použití kľúčov v rámci komunikácie medzi koncovými používateľmi je potrebné využívať protokol SSH (secure shell). Počas prenosov súborov sa využíva secure copy a secure FTP. K základnej vlastnosti SSH patrí je odpamätávanie verejných kľúčov pre budúce použitie. Z pohľadu bezpečnosti dát poskytuje protokol SSH transparentné prenášanie dát s ohľadom na dodržanie integrity dát. V navrhovanom modeli sa využil protokol SSH z dôvodu zabezpečenia terminálového prístupu na vzdialený počítač.

Autorizačné úrovne

Autorizačné úrovne rozdeľujú jednotlivých koncových používateľov do skupín. Delenie do úrovní ovplyvňuje oprávnenia spracovania dát v systéme. Pridelená úroveň definuje aké dáta budú používateľovi zobrazené, v akom zobrazení, aké operácie bude môcť používateľ vykonať s dátami a s kým môže tieto dáta zdieľať. Čím je koncový používateľ dôveryhodnejší, tým sú jeho oprávenia vyššie.

V podnikovom prostredí sú špecifikované tieto autorizačné úrovne:

- klient podniku má najnižšie oprávnenia v rámci podnikových dát, nakoľko prístup klienta do informačného systému firmy je pri možnosti vloženia požiadavky

a pracujú iba s verejnými dátami,

- koncoví používatelia sú zamestnanci firmy, ktorí nezastávajú manažérske pozície a sú im poskytnuté iba dáta potrebné pre ich prácu,
- manažment firmy tvoria zamestnanci, ktorí pracujú s dôvernými a tajnými dátami, avšak neovplyvňujú správanie systému,
- oddelenie informačných technológií je tvorené zamestnancami, ktorí pracujú so všetkými dátami rôznym typov citlivosti, pričom určujú jednotlivé autorizačné úrovne zamestnancom a klientom podniku, teda zasahujú do systému z hľadiska správy.

V univerzitnom prostredí sú definované autorizačné úrovne na základe opísaného Tuncayovho modelu:

- potencionálny záujemca, verejnosť sú základnou a zároveň najnižšou autorizačnou úrovňou, nakoľko do informačného systému môžu vstupovať na základe pridelený verejných hesiel (všeobecné heslá vydané napríklad z dôvodu konferencie), avšak dostupné dáta sú z hľadiska citlivosti verejné, prípadne upravené z dôvodu pôvodu pridelenia autorizačnej úrovne,
- študent univerzity predstavuje druhú úroveň zabezpečenia, keďže pracuje s dátami, ktoré zdieľa v rámci svojej autorizačnej úrovne, pričom sú mu poskytnuté dáta druhého citlivostného stupňa,
- akademickí pracovníci sú treťou úrovňou zabezpečenia a od študentov sa odlišujú vyšším počtom pridelených operácií s dátami ako aj širším okruhom zdieľaní dát, avšak nedisponujú prácou s tajnými dátami,
- manažment univerzity pracuje s predchádzajúcimi úrovňami, a zároveň jeho práva navyššuje práca s tajnými dátami,
- oddelenie informačných technológií pracuje so všetkými typmi dát, pričom určuje jednotlivé privilégiá a možnosti spracovania dát pre predchádzajúce autorizačné úrovne.

Stanovením autorizačných úrovní je bližšie charakterizovaná prepojenosť medzi klasifikáciou dát a koncovými používateľmi systému.

Riešenie zobrazenia uložených dát na základe autorizačnej úrovne je uvedené vo vytvorenom algoritme pre zobrazenie uložených dát.

Algoritmus pre zobrazenie uložených dát na základe autorizačnej úrovne

```
public List<string> GetFiles()
{
    publicPath = Settings.Default.PublicPath;
    confidentialPath = Settings.Default.ConfidentialPath;
    internalPath = Settings.Default.InternalPath;
```

```
    List<string> listOfFiles = new List<string>();
    if (Directory.Exists(publicPath))
        {
         string[] fileEntries = Directory.GetFiles(publicPath);
         foreach (string fileName in fileEntries)
         {
          listOfFiles.Add(Path.GetFileName(fileName));
         }
        }
        if (Directory.Exists(internalPath))
        {
         string[] fileEntries = Directory.GetFiles(internalPath);
         foreach (string fileName in fileEntries)
         {
          listOfFiles.Add(Path.GetFileName(fileName));
         }
        }
        if (Directory.Exists(confidentialPath))
        {
         string[] fileEntries = Directory.GetFiles(confidentialPath);
         foreach (string fileName in fileEntries)
         {
          listOfFiles.Add(Path.GetFileName(fileName));
         }
         }
        return listOfFiles;
}
```

Šifrovací systém

Na základe teoretických východísk prebehlo testovanie uvedených algoritmov pre šifrovanie. Výsledky testovania rozhodli za najvhodnejší systém využiť rozšírenú hashovaciu funkciu SHA. Hlavnou výhodou bola bezpečnosť algoritmu spočívajúca vo vytvorení hashu fixnej dĺžky (označované aj ako miniatúra). SHA vychádza z navrhnutej metodiky a spĺňa protokoly navrhnuté NIST a FIPS.

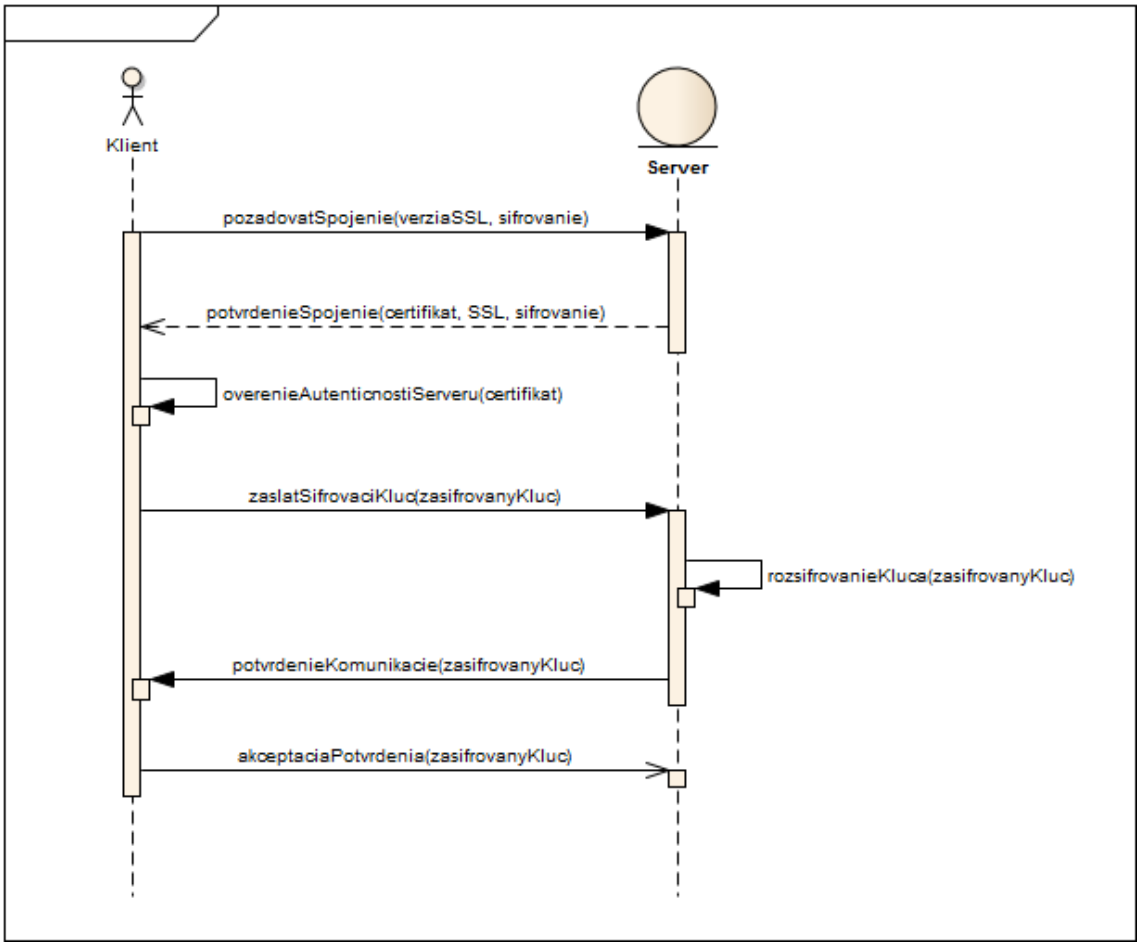
Základom výberu tohto algoritmu bola vysoká dosiahnuteľnosti dodržania integrity dát a podpora kontroly integrity súborov. Rozšírená hashovacia funkcia SHA je využitá pri protokole SSH a SSL. Na základe testovania a uvedených východísk odporúčam SHA pre využitie do podnikového aj univerzitného prostredia.

TLS

Protokol TLS predstavuje vrstvu pre zabezpečenie komunikácie, a teda kryptografický protokol. Napriek tomu, že v teoretických vychodiskách je uvedené doroučenie na protokol SSL, v rámci tejto práce sa využil protokol TLS. Protokol TLS je

nasledovníkom protokolu SSL. Protokol SSL plne podporuje šifrovací systém SHA, pripojenie autentizačného kódu (MAC kód) k ukladanému súboru a jeho šifrovanie.

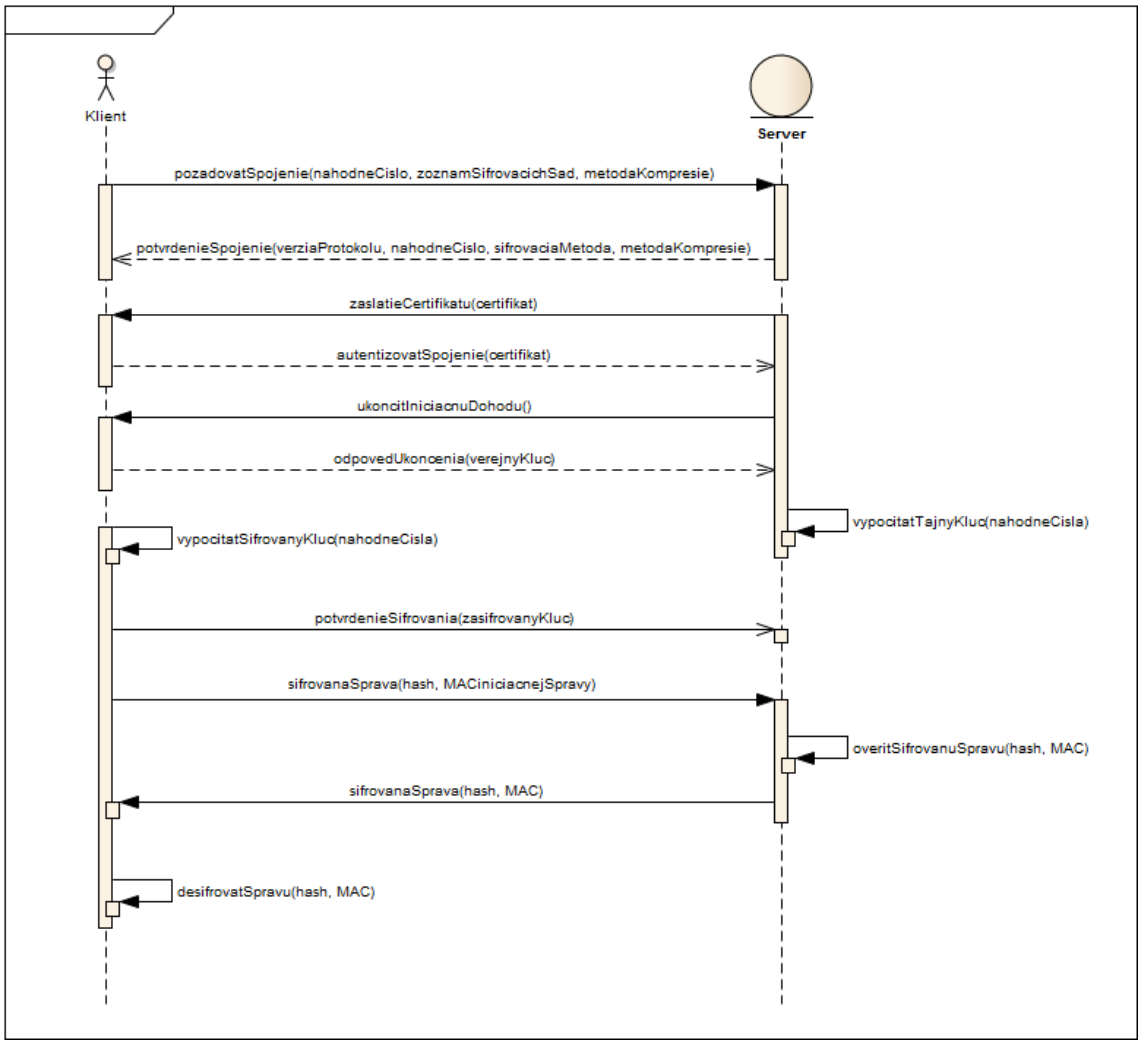
Pre zdôvodnenie výberu protokolu je uvedená komunikácia medzi klientom a serverom z pohľadu oboch protokolov pomocou využitia sekvenčného diagramu na obrázku 12 a obrázku 13.



Obr. 12: Inicializácia spojenia medzi klientom a serverom pri využití protokolu SSL

TLS aj SSL protokol poskytujú šifrovanie dát a autentizáciu medzi aplikáciami a servermi. Zraniteľnosť pri použití oboch protokolov je možné overiť využitím aplikácie POODLE. Na základe výsledkov testovania je protokol SSL považovaný za málo bezpečný pre podnikové prostredie. Pokiaľ podnik chce využívať SSL protokol, tak je potrebné využiť aj iné protokoly ako napríklad IMAP. Pre overenie zabezpečenia týchto protokolov bol využitý taktiež beast attack (útok beštie), ktorý úplne zlomil stránky bežiace pod protokolom SSL vo verzii 3 a pod protokolov TLS verzie 1. Preto je potrebné pri použití protokolu TLS využívať aktuálnu verziu tak ako aj v podnikovom, tak aj v univerzitnom prostredí.

HTTPS



Obr. 13: Inicializácia spojenia medzi klientom a serverom pri využití protokolu TLS

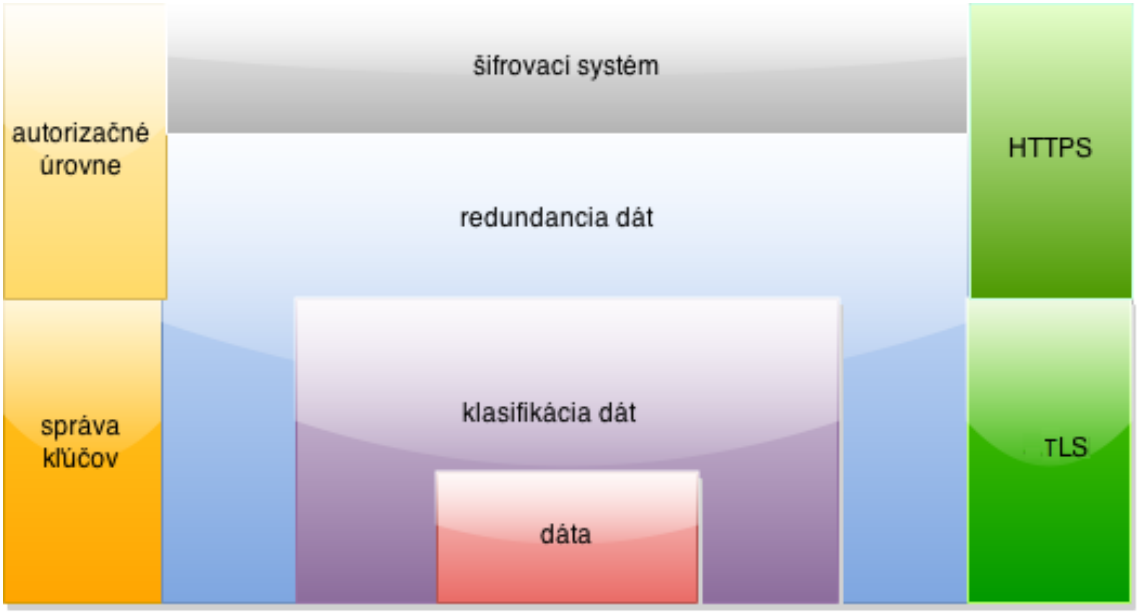
Posledným základným protokolom komunikácie je protokol HTTPS. V návrhu architektúry tento protokol využíva šifrovací systém SHA a kryptografický protokol TLS. Protokol HTTPS je vhodný pre zvýšenie bezpečnosti práce v informačnom systéme v podniku aj v univerzite, nakoľko je určený predovšetkým na dynamický obsah, ktorý nie je verejne dostupný. V rámci spojenia cez tento protokol nie je možné vytvárať viacero virtuálnych webových serverov na jednej IP adrese. K jeho nevýhodám patrí spomalenie odozvy systému.

Nastavenie latencie

Na základe teoretických východísk je vhodné určiť dĺžku latencie v rámci komunikácie, avšak na základe testovania sa potvrdil opak, a teda určenie latencie spôsobuje spomalenie systému a poskytuje nízku bezpečnosť. Keďže navrhnutý systém má mať pomerne dobrú odozvu, zaviedla sa neobmedzená latencia, a teda neobmedzovanie sedenie koncového používateľa.

Kompatibilita blokov architektúry

Uvedené bloky sú zhrnuté do jednej schémy, pričom sú farebne označené bloky, ktoré sa najviac ovplyvňujú a spolupracujú. Schému je uvedená na obrázku 15. Z uvedenej schémy vyplýva aj dôležitosť jednotlivých blokov, základ architektúry a celkový pohľad na architektúru vzhľadom k jednotlivým vrstvám.



Obr. 14: Bloky navrhnutej architektúry

Návrh infraštruktúry

Návrh infraštruktúry je zovšeobecnený pre podnikové aj univerzitné prostredie, pričom bol verifikovaný v rámci univerzity. Pre hĺbkovú analýzu a overenie navrhnutého riešenia bol využitý vlastný hardvérov.

Hardvérové komponenty

Hardvér dátového úložiska je zvolený vzhľadom k zníženiu nákladov, aby bola takto potvrdená využiteľnosť navrhnutého riešenia aj pre strednú firmu (prípadne malý podnik). Základom dátového úložiska sú dve jednoprocesorové servery Fujitsu Primergy RX100S8. Výber typu serveru ovplyvnila kompatibilita s dátovými zariadeniami univerzity a pomer cena/technické parametre. Počet serverov je ovplyvnený možným výpadkom. Jeden server je primární, druhý je sekundárny v prípade vypadnutia primárneho servera. Ideálny stav je pri využití troch serverov, pretože v okamihu, keď sú tri servery a vypadne jeden, je stále k dispozícii jeden sekundárny server. Nakoľko nákup hardvéru bol platený z projektu, nebolo možné zakúpiť ďalší server. (Priščáková a Salák, 2013)

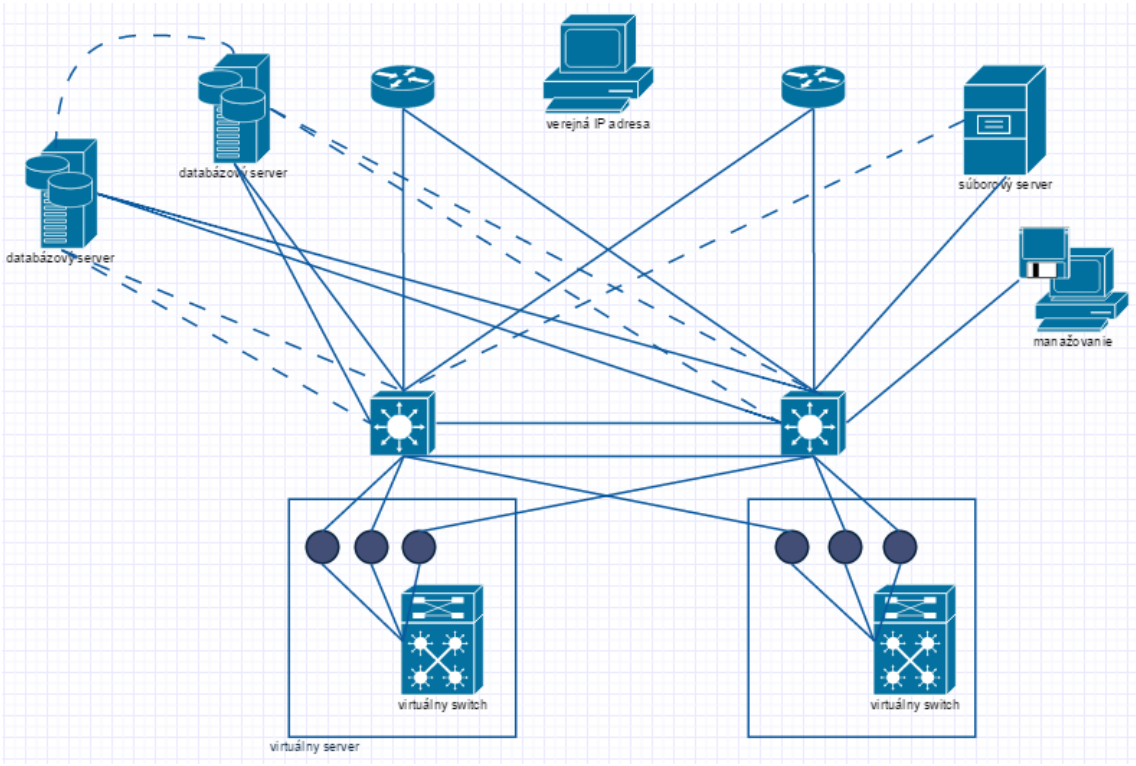
Hlavné dátové úložisko pozostáva z dvoch dátových úložísk, ktoré boli zostrojené na základe komponentov uvedených v tabuľke 1.

Tabuľka 1: Zoznam komponentov vlastného serveru v dátovom úložisku

Názov komponentu	**Cena komponentu**
Diskové pole SATA III 1 TB	2055 Kč
Chladič pre procesor Noctua NH-L9i	996 Kč
Operačná pamäť Patriot Viper 3	8233 Kč
Počítačová skriňa 2U	9707 Kč
Procesor INTEL Quad-Core Xeon E3-1230L	6144 Kč
Grafická karta Zotac GT 610 PCI-Express 512MB	1413 Kč
Sieťová karta Intel Gigabit CT	638 Kč
Základná doska ASRock Z97 Extreme4	3211 Kč

Výsledná cena jedného serveru je 36507 Kč. Vzhľadom k porovnaniu výkonu dátového úložiska s konkurenciou na trhu bolo zistené, že zostavené úložisko je lacnejšie o 20000 Kč. Kapacita jedného úložiska je 3 TB. Požiadavky na napájanie sú 450 W pre server a 560 W pre dátové úložisko. Požiadavky na celkovú klimatizáciu sú 460 W.

Uvedené servery boli zapojené podľa schémy návrhu infraštruktúry. Návrh infraštruktúry je uvedený na obrázku 15. Prístup do siete poskytuje verejná IP adresa. Následne sú použité pre bezpečnosť dát 2 routery a switche. Tým je zabezpečená ochrana pred prípadným výpadkom jedného serveru. K hlavným komponentom schémy patria dátové úložiská, a teda 2 servery, ktoré navzájom spolu komunikujú z dôvodu redundancie dát, a zároveň sú prepojené cez switche s aplikačnými servermi (fyzické stroje slúžiace pre virtualizovanie serverov a implementáciu aplikácií) pričom zahrňujú podmienku vyrovnania záťaže. Pre manažovanie siete slúži klient. Navrhnutá schéma spĺňa podmienky bezpečnosti uvedené v navrhnutej metodike. (Priščáková, Rábová a Salák, 2013)



Obr. 15: Schéma návrhu infraštruktúry

Implementácia a testovanie technológií

Verifikácia rámcovej metodiky prebehla testovaním aktuálne dostupných technológií zameraných na riešenie integrity dát a open-source riešenie.

Implementácia bola rozdelená do týchto častí:

- implementácia virtualizovaného prostredia,
- úprava hardvéru,
- implementácia súborového systému.

Implementácia virtualizovaného prostredia

Pre zníženie vstupných nákladov pri zavedení cloud computingu pre strednú firmu (ale aj univerzitu, prípadne malú firmu) bola použitá open-source virtualizačná technológia KVM. Základom implementácie je príkaz *virt-install* v príkazovom riadku. Tento príkaz vytvára nové virtuálne stroje s podporou zoznamu možností príkazového riadku. Pre implementáciu je možné využiť aj príkaz *virt-manager*. Rozdiel medzi týmito príkazmi spočíva v tom, či je dostupný počítač pre manažovanie, alebo nie. Pri inštalácii bol využití príkaz virt-install, nakoľko inštalácia prebiehala priamo na server.

Pre plné využitie možností KVM boli implementované balíčky *virt-viewer*, *qemu-kvm* a samotné KVM príkazom:

yum install kvm virt-viewer qemu-kvm

Pre zabránenie prípadnej chyby pri inštalácii by mohol byť použitý aj jednotný príkaz inštalácie balíčkov:

yum groupinstall 'Virtualization'

Príkaz virt-install poskytuje podporu grafiky pri inštalácii hosťujúceho operačného systému. Je to dosiahnuté použití QEMU. V prípade zakázanej podpory grafiky by bol použitý štandardný textový inštalačný program. Príkaz virt-install bol spustený ako root s dosiahnutím prijatia širokej škály argumentov príkazového riadku. Tieto argumenty boli neskôr využité pre určenie informácií o konfigurácii vytvorených virtuálnych strojov. Pre zadáveni argumentov bolo potrebné dohliadnuť na kapacitu RAM a voľné miesto na disku.

Pre vytvorenie KVM virtuálneho stroja konfigurovaného pre Windows XP s 8 GB diskovým obrazom, priradenej pamäti RAM o veľkosti 1024 MB, konfigurovaním CD zariadenia pre inštalačné média a použitím VNC zobrazovej konzoly bol použitý tento príkaz (Prišťáková, 2014):

virt-install –name myWinXP –ram 1024 –disk path=/tmp/winxp.img,size=8 –network network:default –vnc –os-variant winxp –cdrom /dev/sr0

Pre klonovanie stroja bola použitá technológia DRBL (diskless remote boot in linux) obsahujúca open-source softvére Clonezilla server edition.

Úprava hardvéru

Prvým krokom bolo konfigurovanie hardvéru, kde boli vyskúšané šifrovací systém RSA a hashovacie funkcie MD5 a SHA. Konfigurácia bola prevedená cez manažéra konfigurácie hardvéru. Pri každom použitom systéme boli prevedené testy. Kolízia nastala v systéme RSA (overenie podľa (Boneh a Venkatesan, 1998)). Hashovacie funkcie boli bez problémové, ale nakoľko MD5 je radená k zastaralým funkciám a bola prelomená, bola výsledná použitá hashovacia funkcia SHA.

Z teoretických východísk vyplýva spomalenie rýchlosti prenosu dát pri použití cloud computingu. Pre riešenie tohto problému bol zostavený RAMdisk. Veľkosť RAMdisku bola 10 GB a samotná implementácia bola prevedená týmto príkazom:

mkdir /tmp/ramdisk; chmod 777 /tmp/ramdisk mount -t tmpfs -o size=10G tmpfs /tmp/ramdisk/

Pre testovanie rýchlosti bola prevedená operácia zápisu 5 GB súboru. Počet testovaní bol 50. Priemerná rýchlosť bola 1563 MB/s, čo je vyššie než bežný HDD disk. Táto hodnota je porovnateľná s hodnotou SSD diskov (Henthorn, 2014).

RAMdisk z hľadiska bezpečnosti nie je optimálnym riešením, avšak jeho bezpečnosť je možné zvýšiť duplikáciou po sieti na ďalšie stroje, alebo oneskorenou synchronizáciou s SSD diskom.

Implementácia súborového systému

Pre riešenie integrity dát bol zvolený súborový systém ZFS. Kľúčovou vlastnosťou ZFS je integrácia konceptov súborového systému a správy zväzkov. ZFS je navrhnutý pre maximálnu integritu dát, dátové snímky, viacero kópií a kontrolné súčty

dát. Využíva softvér replikácie dátového modelu, známeho ako RAID-Z (RAID – je súhrnný termín označujúci rôzne schémy ukladania dát používajúce viacero diskov na rozdeľovanie alebo replikáciu dát medzi jednotlivými diskami). RAID-Z poskytuje redundantne podobný hardvér RAID, ale je navrhnutý tak, aby sa zabránilo zápisu dát korupcie a prekonaniu niektorých obmedzení hardvéru RAID (Rouse, 2012).

ZFS je založený na virtuálnych dátových oblastiach nazývaných zpools. Jeden zpool, ktorý tvorí základ systému ZFS, môže pozostávať z mnohých fyzických zariadení. Zpool pozostáva z virtuálnych zariadení (vdevs), ktoré sú zas zložené z blokových zariadení ako súbory, partície, alebo skutočné fyzické zariadenia. Blokové zariadenia v rámci vdev môžu byť nastavené rôznymi spôsobmi v závislosti od potrieb a dostupného miesta. Dynamické rozloženie záťaže (Dynamic striping) maximalizuje priepustnosť systému tým, že po pridaní nového fyzického disku naň automaticky presunie časť dát a tým odľahčí ostatné fyzické disky od obsluhy operácií nad danými dátami (Ayad a Dippel, 2011).

ZFS sa snaží dátovými presunmi medzi fyzickými zariadeniami zabezpečiť optimálne rozloženie záťaže. V systéme ZFS manipulácie so súborovými systémami (partíciami) sú podstatne jednoduchšie ako v bežných súborových systémoch. Namiesto fyzického premiestňovania množstva dát sú do veľkej miery realizované len modifikácie príslušných odkazov. Čas a zložitosť vytvárania novej partície v rámci ZFS sú približne ekvivalentné vytváraniu nového adresára v niektorých bežných súborových systémoch.

Testovaním bolo zistené, že pri dosiahnutí 70 percentnej obsadenosti určenej veľkosti ZFS dochádza k spomaleniu až k zmrazeniu systému. Pri dosiahnutí 95 a viac percentnej obsadenosti súborového systému sa začína súborový systém výkonnostne stávať takmer nepoužiteľným.Z tohto dôvodu je potrebné pri použití ZFS dbať na možnosti kapacity. Na druhej strane z pohľadu integrity je ZFS pomerne optimálna. Pri testovaní bol použitý príkaz zo zápisu 5 GB súboru, pričom bola testovaná verzia výpadku siete, výpadku disku a korektného uloženia. V budúcnosti by bolo vhodné využiť lepší systém pre zabezpečenie integrity dát, a to GlusterFS, nakoľko umožňuje vysokú škálovateľnosť z pohľadu riešenia integrity dát.

Zhrnutie podkapitoly

Verifikácia metodiky bola prevedená v troch etapách. V úvodnej časti bol definovaný hrubý návrh architektúry pre dodržanie bezpečnosti dát. Návrh architektúry obsahoval základné bloky, ktoré je potrebné doržať pre zabezpečenie komunikácie medzi koncovým používateľom a serverom, ako aj koncovými používateľmi navzájom. Základom architektúry bolo stanovenie typu architektúry klient-server.

V druhej časti bola architektúra aplikovaná na návrh infraštrutúry a prepojenie hardvérového a softvérového riešenia. Návrh infraštruktúry sa zameriaval na zjednotenie oboch implementovaných prostredí, pričom bolo docielené zníženie vstupných nákladov na vytvorenie vlastného dátového úložiska. Splnením tohto cieľa boli

poukázané nové na možnosti vytvorenia vlastného úložiska aj pre malé a stredné podniky so zámerom o odprostrenie od poskytovateľa cloudu.

V záverečnej časti boli zhrnuté samotné kroky implementácie a testovanie technológií. Výsledky poukázali na nové možnosti rozpracovania navrhnutej metodiky, ktoré sú uvedené v diskusii. Verifikácia metodiky bola prispôsobená podnikovému a univerzitnému prostrediu. Jednotlivé rozdiely sa definovali v každom kroku verifikácie. Z uvedených výsledkov vyplýva, že výber implementovaného prostredia ovplyvňuje aj spôsob zabezpečenia dát ukladaných do cloudu.

3.4 Návrh riešenia dostupnosti

Obsahom tejto podkapitoly je riešenie dostupnosti cloudu s ohľadom na možnosti využitia alternatívnych energetických zdrojov. Táto prípadová štúdia bola vytvorená na základe fyzikálnych poznatkov a dnešného trendu využitia hybridných solárnych systémov (Prišč áková a Rábová, 2013).

Alternatívne energetické zdroje sú dnes považované za riešenie energetickej závislosti ľudstva v budúcnosti. Solárna energia je považovaná za dnešný trend v oblasti alternatívnych zdrojov. Pre zachytenie žiarení slúži solárny systém (Hamilton, 2012). Bohužiaľ, solárne systémy sa bez doplnkového zdroja nezaobídu, nakoľko nie sú schopné v stredoeurópskych podmienkach zabezpečiť ekonomicky efektívnym spôsobom celú svoju spotrebu (Iliaš, Guschlbauer-Hronek, Benesch a Bayer, 2006). Na základe aktuálnych poznatkov môžem tento fakt čiastočne vyvrátiť.

Pre výpočet slnečnej energie dopadajúcej na plochu $1m^2$ našej Zeme sa opieram o fyzikálne základy. Zem obieha okolo Slnka po eliptickej trajektórii. Ohniskom dráhy obehu Zeme je práve Slnko. Keďže trajektória obehu Zeme má tvar elipsy, je potrebné rátať so zmenou vzdialenosti Zeme a Slnka. Pri prechode atmosférou slnečné lúče uberajú na svojej intenzite. Celkový svietivý výkon Slnka je označovaný termínom luminozita (L) . Na základe vzťahu medzi luminozitou a vzdialenosťou Zeme od ohniska, viem vypočítať intenzitu žiarenia. Je dôležité poznamenať, že Zem sa môže nachádzať v dvoch polohách v rámci vzťahu so Slnkom. Apohélium je poloha Zeme, keď je najviac vzdialená od Slnka. Najkratšia vzdialenosť je označovaná ako perihélium. Meniacu sa vzdialenosť vzhľadom na trajektóriu je vhodné vyjadriť výpočtom excentricity na základe doposiaľ uvedených konštánt.

Aby bol model prispôsobený reálnym podmienkam je potrebné rátať aj s uhlom, ktorý je tvorený spojením ľubovoľného bodu na trajektórii Zeme so Slnkom a spojením Slnka a Zeme, keď sa nachádza v perihélium. Tento uhol je označovaný gréckym znakom φ.

Zatiaľ, čo priame slnečné žiarenie úzko súvisí s polohou Zeme obehu trajektórie okolo Slnka, difúzne žiarenie ovplyvňuje difúzny faktor vonkajšieho prostredia. Priamy slnečný lúč pri dopade na zemský povrch prechádza cez atmosféru. Jednotlivé oblaky lámu slnečné žiarenie, a tak dochádza k rozptyľovaniu lúču. Pri lome svetla sa uplatňuje Snellow zákon. Pri dvoch odlišných prostrediach sa pomer sínusu uhla dopadu a sínusu uhla lomu nazýva relatívny index lomu. Známe sú dva typy

lomu svetla v závislosti od hustoty prostredia. Ak svetelný lúč prechádza z opticky redšieho prostredia do opticky hustejšieho, dochádza k lomu od kolmice. V opačnom prípade je tento lom ku kolmici.

Ďalším aspektom pri výpočte difúzneho žiarenia je dopad slnečných lúčov na nerovnomerný zemským povrch. Zem je tvorená súšou a vodnými plochami. Pri styku so súšou sa lúče odrážajú od pohorí. Vzniká takto jedna z častí difúzneho žiarenia. Vodné plochy sú sprevádzané vyparovaním vody, čím sa tvorí vodná para. S týmto javom súvisí difúzny odpor vzhľadom k prostrediu. Vzduch má najnižší difúzny odpor.

Pri pôsobení difúzneho žiarenia je dôležité zahrnúť aj uhol sklonu solárneho kolektora. Pri vertikálnej polohe sa kolektor nachádza v sklone. Žiarenie, ktoré dopadá na jeho plochu, je iba čiastočné. Najvyšší energetický zisk je pri horizontálnom umiestnení kolektora. Jeho uhol sklonu je nulový, teda plocha slnečného panelu je plne dostupná prijímaniu difúzneho žiarenia.

Základ výpočtov sa opiera o hodnotu luminozity Slnka, $L_0 = 3,842 \times 10^26$ W. Intenzita slnečného žiarenia sa označuje I_0 . Pre jej matematické vyjadrenie je potrebné do rovnice zahrnúť aj vzťah polohy Zeme a Slnka označovanej ako vzdialenosť r. Hodnota intenzity slnečného žiarenia je priamo úmerná luminozite Slnka a nepriamo úmerná zmene vzdialenosti medzi Slnkom a Zemou.

$$I_0(r) = \frac{L}{4^2} \tag{8}$$

V tomto vyjadrení je vzdialenosť konštantná hodnota, čo však nie je správne. Zem sa pohybuje po elipsovitej dráhe. Zem v ponímaní tejto elipsy prechádza do rovnodennosti a vytvára dve ohniská. Vzdialenosť ohniska od stredu elipsy určuje hodnota excentricity elipsy ϵ.

Vyjadruje sa nasledovne:

$$\epsilon = \sqrt{a^2 - b^2} \tag{9}$$

Po vyjdrení zmeny vzdialenosti Slnka od stredu trajektórie Zeme, je potrebné vyjadriť vzdialenosť medzi Zemou a Slnkom. Pri tomto vyjadrení je dôležité zahrnúť aj vzdialenosť pri rovnodennosti označenú ako r_0. Táto vzdialenosť je priamo úmerná vzdialenosti Zeme od Slnka s ohľadom na uhol φ. O tomto uhle môžem povedať, že je nepriamo úmerný so siderickým rokom. S uhol súvisí aj doba, ktorá uplynie od prechodu cez deň rovnodennosti označená písmenom t. Z uvedeného vyplýva nasledujúci vzťah:

$$r(\varphi) = \frac{r_0}{1 + \epsilon cos\varphi} \tag{10}$$

V tomto vzťahu je známa aj závilosť excentricity od vzdialenosti. Tento vzorec rozviniem a aplikujem znalosti o dvoch ohniskách elipsy. Pri závislosti Zeme a Slnka sú tieto ohniská označené ako perihélium a apohélium. Po úprave rovnice, vzniknú dve rovnice pre výpočet vzdialenosti v oboch ohniskách elipsy.

$$r_{apohelium} = \frac{r_0}{1-\epsilon}, r_{perihelium} = \frac{r_0}{1+\epsilon} \tag{11}$$

Uvedené vzorce boli aplikované do základného vzorca pre výpočet slnečnej intenzity.

$$I_0(r) = \frac{L}{4\pi r^2} = \frac{L}{4\pi r_0^2}(1+\epsilon cos\varphi)^2 = \frac{L}{4\pi r_0^2}(1+2\epsilon cos\varphi) \tag{12}$$

Uvedený vzťah platí pre umiestnenie solárneho kolektoru v horizontálnej rovine, nakoľko ide o najefektívnejšie spracovanie solárneho žiarenia.

Na solárny kolektor okrem priameho žiarenia pôsobí aj difúzne žiarenie. Pri horizontálnej rovine kolektora je toto žiarenie priamo úmerné priamemu žiareniu. Do vzorca je potrebné zahrnúť aj vonkajšie vplyvy rozptylu, a preto zavádzam konštantu difúzneho faktoru μ.

$$I_d = I_0\mu \tag{13}$$

Konštantu difúzneho faktoru vypočítam podľa tohto vzorca:

$$\mu = 0,095 + 0,04sin[(360/365).(t-100)] \tag{14}$$

Aplikovaním týchto druhov žiarení dostávame vzťah pre výpočet celkového slnečného žiarenia počas jasného dňa v jednotkách W/m^2.

$$I = I_d + I_0 \tag{15}$$

Z uvedeného vzorca sa vypočíta celkové slnečné žiarenie dopadajúce na 1 m^2.

Simulácia výpočtu celkového slnečného žiarenia

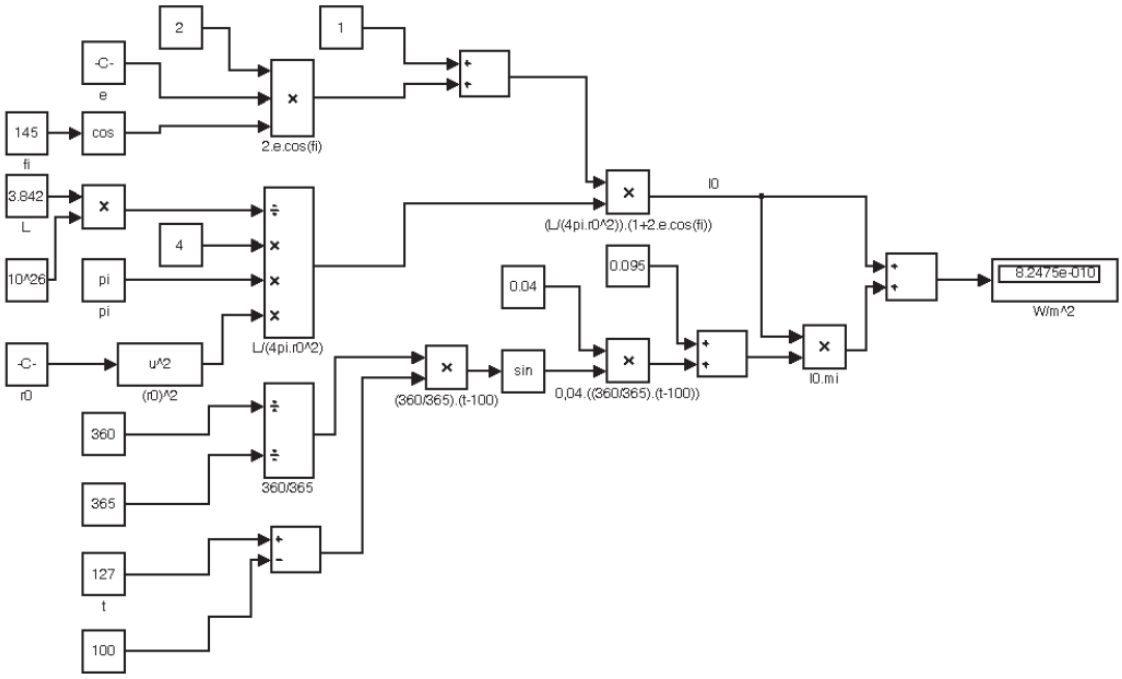
Simulácia výpočtu celkového slnečného žiarenia bola prevedená transformovaním vyššie uvedených rovníc do prostredia MATLAB Simulink. Simulácia dokázala určiť výhodnosť navrhovaného hybridného solárneho systému. Avšak, simulovaný model neráta so znížením produktivity energie po určitom období používania a počas zimných období. Po aplikovaní týchto negatívnych faktorov sa systém stáva nevýhodný. (Priščáková a Rábová, 2013)

Schéma simulácie je znázornená na obrázku 16. Výstup simulácie zaznamenávam prostredníctvom bloku Display. Vstupné hodnoty konštánt sú fiktívne vzhľadom k umiestneniu hybridného solárneho systému. (Priščáková a Rábová, 2013)

Návrh hybridného solárneho systému

Pre daný návrh bol zvolený server s požadovaným príkonom 750 W. Ako príklad uvádzam server od spoločnosti IBM x3550M4, ktorý bol pôvodne plánovaný k zakúpeniu v rámci riešenia projektu, avšak jeho cena bola príliš vysoká.

Server vo firmách funguje nepretržite v každú hodinu dňa, teda celoročne. Pri využití solárneho systému je potrebné si uvedomiť polohu umiestnenia tohto serveru vzhľadom na zemepisné súradnice. V tejto modelovej situácii bol server umiestnený



Obr. 16: Schéma výpočtu celkového slnečného žiarenia

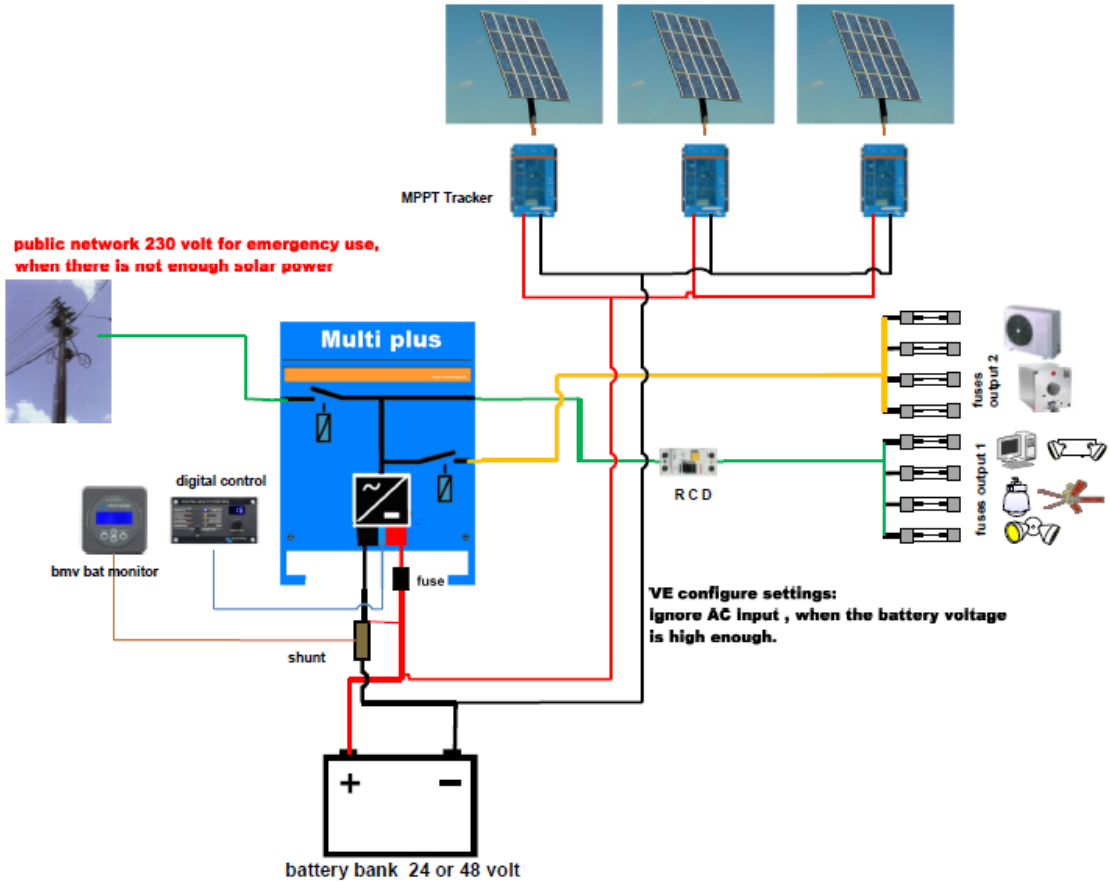
v meste Brno (Česká republika). Brno leží v strednej Európe, a teda intenzita slnečného žiarenia a dĺžky svietivosti je ovplyvnená ročným obdobím. Z tohto hľadiska vyplynulo plné využívanie systému počas mesiacov máj až september. Počas ostatných mesiacov sa systém pripájal na sekundárny zdroj energie, a teda elektrický prúd. Pre solárny systém bolo dôležité určiť aj jeho umiestnenie s čím súvisí typ strechy. Pre hybridný systém bola zvolená rovná strechu bez tienenia, pričom orientácia je na juh a sklon je 30 stupňov. Tieto údaje mi poskytla univerzita MENDELU a odzrkadľujú budovu fakulty PEF.

Pre určenie svietivosti v danej lokalite bol kontaktovaný Hydrometeorologický ústav v Brne, ktorý poskytol dáta v rámci jednoltivých dní (Český hydrometeorologický ústav, 2013). Nakoľko pre výskum boli potrebné podrobnejšie dáta (rozpis v jednotlivých minútach), poskytnuté dáta neboli využité. Podrobnejší rozpis svietivosti bol spoplatnený ústavom v Brne, a keďže v rámci prípadovej štúdie a daného projektu sa neočakávali takéto investície, nebolo možné dáta zakúpiť.

Pri zostavovaní schémy systému na obrázku 16 bola nadviazaná spolupráca s firmou NEOSOLAR, Jihlava. Keďže ide o odborníkov v oblasti solárnej energetiky, upozornili ma na niektoré problémy s uvedeným riešením a možnosti ich odstránenia pomocou nových komponentov určených pre tvorbu hybridného solárneho systému.

Pre uchovávanie solárnej energie boli zavedené uzavreté vetrané olovené batérie. Spoločnosť NEOSOLAR odporučila za najvhodnejšie batérie Hoppecke OPzS. Ich veľká výhoda pre navrhnuté riešenie spočíva v dlhej životnosti v rámci cyklickej prevádzky. Tieto batérie disponujú cirkuláciou elektrolytu, čo znižuje nabíjací faktor.

Nakoľko existuje niekoľko typov uvedených batérií, za najvhodnejší typ bol zvolilený typ 8 (OPzS 1220). Batérie pracujú pri napätí 2 V a ich celková kapacita je 1063 Ah pri C24 (vybíjanie 24 prúdom 44,3 A).



Obr. 17: Schéma riešenia hybridného solárneho systému

Z dôvodu výparov z batérií, a tak dosiahnutiu zníženia údržby batérií, spoločnosť Hoppecke ponúka rekombinačný systém AquaGen (Hoppecke, 2012). Účinnosť rekombinácii je až 99 percent. Cieľom tohto systému je nasávať plyny (vodík, kyslík), ktoré vznikajú pri rozklade vody v batérii. Rekombinátor je namontovaný na batériu ako externá súčasť, čím sa zníži nárast teploty v batérii. Keďže kapacita batérií je vysoká, je potrebné použiť typ V (Hoppecke, 2012).

Nabíjanie batérií je zabezpečené pomocou solárneho regulátoru MPPT od spoločnosti BlueSolar. Nabíjací prúd je až do 70 A a fotovoltaické (FV) napätie do 150 V. Maximálna účinnosť regulátora je 98 percent. Tento regulátor slúži na regulovanie nižšieho nominálneho napätia na vyššie nominálne napätie FV. Regulátor sa automaticky prispôsobí na 12 V, 24 V, 48 V napätia batérie. Jeho výhodou je disponovanie detekcie čiastočného tienenia a zvýšenie energetického zisku až o

30 percent v prípade mierneho tienenia oblakmi pri stálej intenzite svetla (Victron energy, 2012). Medzi solárnymi panelmi a regulátorom je bleskoistka a istič C40.

Aby sa vyrobila potrebná energia, je potrebné zostaviť hybridný solárny systém z 24 solárnych panelov od spoločnosti IBC so špičkovým výkonom 240 Wp. Nominálne napätie panela je 24 V. Výrobca odporúča tento panel použiť pre priemyselné budovy, veľkoplošné strechy. Efektívnosť solárneho panelu sa po 12 rokoch zníži na 90 percent a po 25 rokoch klesá na 80 percent (Neosolar, 2012).

Základom solárneho systému je centrálna jednotka MultiPlus. Táto jednotka funguje ako aj ako nabíjačka, aj ako menič. V prípade meniča vystupuje vo vzťahu napojenia vlastného spotrebiča z batérií. Ako nabíjačka funguje v prípade zníženej intenzity svietivosti, kedy dobíja batérie zo sieťového prúdu.

Ak dôjde k poklesu napätia v akumulátoroch pod nastavenú hodnotu, MultiPlus dobije energiou akumulátory. Na dobíjanie sa využije energia zo siete. Jednotka MultiPlus dobíja akumulátory dovtedy, pokiaľ nedosiahnu inicializovanú nastavenú hodnotu. Pri nastavení je dôležité určiť hodnotu energie v akumulátoroch tak, aby ostalo dostatok kapacity aj pre uloženie vyrobenej energie. Takéto nastavenie bude maximálne uprednostňovať využitie solárnej energie pred pripojením na elektrický prúd.

Vybíjanie akumulátorov sa predpokladá maximálne do polovice percent celkovej kapacity, teda 1063/2 Ah (Neosolar, 2008). Vďaka paralelnému fungovaniu môžem povedať, že výkon je takmer neobmedzený. MultiPlus nahrádza napätie zo siete v prípade výpadku sieťovej energie, a tak rieši možné problémy s bezproblémovým chodom servera. K nemenej výrazným výhodám jednotky patrí aj možnosť vzdialeného ovládania pomocou Digital multicontrol panel 200/200 A. Pre vzdialené sledovanie sa využije Global remote 2, na ktorý sa pripája sledovač batérií.

Pri 750 W záťaži sa spotrebuje denne 18000 Wh, čo je 375 Ah pri napätí 48 V. Denná výroba FV poľa v lete je približne 450 Ah pri 48 V. Prebytky vykompenzujú straty nabíjaním kabeláže a podobne. Predpokladané solárne pokrytie v ročnom priemere je 60–70 percent. V lete ide o stopercentné solárne pokrytie a v zime je to približne 25–30 percent bez zahrnutia snehovej pokrývky.

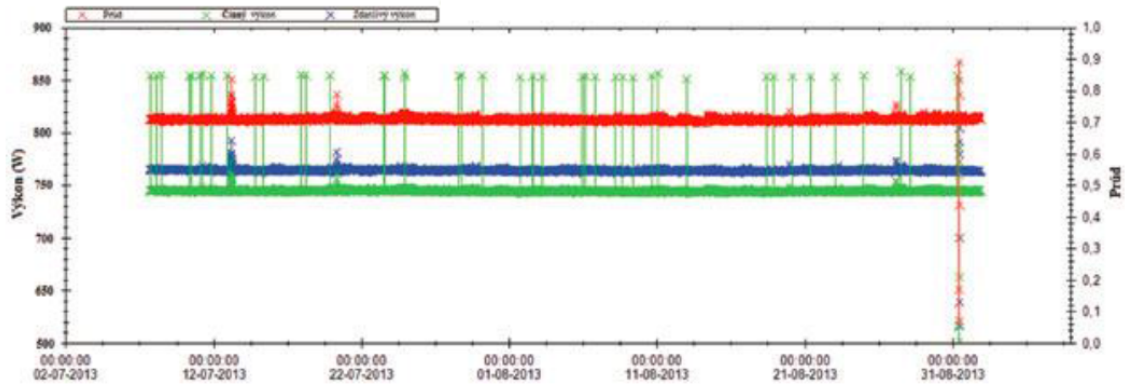
Celková suma tohto riešenia aj s kompletným riešením prepojenia pomocou káblov, elektrorozvádzačov, stojanov, držiakov, montážou, dopravou, sprevádzkovaním, nastavením a zaučením je 811523 Kč.

Prípadová štúdia zavedenia hybridného solárneho systému

Pre konečné zhodnotenie využitia hybridného solárneho systému ako zdroj pre server boli prevedené merania na poskytnutom univerzitnom serveri. Pre relevantnosť výsledkov projektu boli vykonané merania servera, ktorý mi pridelil Ústav informatiky MENDELU. V pôvodnom riešení projektu bol zvolený merač spotreby servera kliešťový wattmeter C.A. F607. Avšak konzultácie poukázali na jeho nevhodnosť a finančnú nevýhodu v pomere cena a dostupné funkcie. Z týchto dôvodov bol využitý vhodný a finančne dostupnejší wattmeter Energy Logger 4000 F.

Softvér Voltsoft mi pomohol vydedukovať správanie servera vzhľadom na jeho spotrebu v jednotlivých obdobiach. Na základe transformácie čísel pomocou tohto

softvéru bol vytvorený diagram s určením prúdu, aktívneho výkonu a zdanlivého výkonu. Nižšia kvalita obrázku je spôsobená problémom s kompatibilitou softvéru Voltsoft. Výsledky boli podrobené analýze a porovnané s výsledkami simulácie v MATLABe.



Obr. 18: Namerané hodnoty univerzitného servera

Ekonomické zhodnotenie prípadovej štúdie

Pre dokázanie efektívnosti, respektíve neefektívnosti hybridného solárneho systému, boli prevedené jednoduché ekonomické zhodnotenie tohto riešenia. Hodnota jednotkovej ceny elektrickej energie bola nastavená na cenu 5 Kč/1 kWh (neboli mi poskytnuté údaje o tarife univerzity). Predpokladaná mesačná spotreba servera je 733 kWh. Suma za túto mesačnú spotrebu činí 3665 Kč. Ročná spotreba má hodnotu 8796 kWh, a teda za túto spotrebu zaplatíme 43980 Kč. Cena tohto hybridného solárneho systému je 811523 Kč. Za spotrebu prostredníctvom verejnej siete by sa za 20 rokov (doba aktívnej funkčnosti solárneho systému stanovená na základe udania výrobcov jednotlivých komponent systému) uhradilo 879600 Kč.

Z tohto faktu vyplýva, že toto riešenie je vhodné aj po ekonomickej stránke, avšak pri výpočte nebola prihladnutá znížená účinnosť solárneho systému po niekoľkých rokoch (predpokladaná doba zníženia účinnosti je po 15 rokoch). Po zavedení týchto parametrov je výsledná suma na zostavenie hybridného solárneho systému vyššia ako útrata za spotrebu univerzitného servera prostredníctvom verejnej siete.

Keďže wattmeter Energy Logger 4000 F svoje údaje uchováva a najvhodnejšie je pre spracovanie dát využiť čo najdlhšie obdobie merania, boli výsledky meraní spracované po dlhšom období. Tieto výsledky poukázali, že predpokladaný príkon servera sa nepotvrdil. Hodnota príkonu bola oveľa nižšia, čo spôsobilo, že po ekonomickom zhodnotení riešenia bolo prepojenie hybridného solárneho systému na tento server radikálne zamietnuté.

3.5 Zhrnutie výsledkov

Výsledkom dizertačnej práce je návrh rámcovej metodiky pre zvýšenie bezpečnosti dát ukladaných do cloud computingu. Navrhnutá metodika vyplýva z modelu zvýšenia bezpečnosti ukladaných dát, odvodenia bezpečnostných pravidiel a identifikácie životného cyklu ukladaných dát.

Model zvýšenia bezpečnosti ukladaných dát je založený na publikáciách NIST 800-52, NIST 800-77, NIST 800-81, NSTISSI 7003 pre integritu a dôvernosť dát, štandarde FIPS 199, publikáciách NIST 800-37, NIST 800-53A pre monitorovanie udalostí. Model pozostáva z bezpečnostných modulov, ktoré obsahujú pridelené povolené funkcie v rámci dodržania životného cyklu ukladaných dát.

Modul *Integrita dát* vyplýva z problému komplexnej realizácie riešenia dodržiavania integrity dát voči životnému cyklu dát. Modul *Vstupné dáta* ovplyvňuje riadenie životného cyklu dát a rieši problém klasifikácie dát, stupňa ochrany a výberu vhodného šifrovacieho algoritmu. Modul *Monitorovanie bezpečnosti* slúži pre neustále sledovanie činností a riadenie konfigurácie a kontrolných informácií súčastí systému. *Klientský modul* stanovuje primerané hodnoty kontroly, ktoré sú uplatnené na koncových používateľoch. Modul *Riadenie účtov* slúži pre riadenie správy účtov, pričom v sebe zahŕňa vytváranie, aktiváciu, úpravu, revíziu, vypnutie a odstránenie účtu. Modul *Riziká zabezpečenia* slúži pre identifikáciu rizík a vytvorenie rizikovej politiky. Modul *Citlivé dáta* aktualizuje posúdené riziká z dôvodu typu citlivosti dát.

Pre formalizáciu metodiky bol použitý *nedeterministický konečný automat a Petriho sieť*. Finálne stanovenie krokov rámcovej metodiky bolo zamerané na prepojenie určeních bezpečnostných pravidiel s implementáciou cloud computingu v podnikovom a univerzitnom prostredí. Navrhnutá metodiky pozostáva z 15 krokov, ktoré v sebe zahŕňajú analýzu prostredia, stanovenie aktérov, identifikovanie zdrojov dát, nastavenie oprávnení koncových používateľov, definovanie operácií, určenie rizikových procedúr, definovanie hranice ochrany dát, stanovenie rizikovej politiky, konfigurácciu dátového úložiska, aplikovanie navrhnutej infraštruktúry siete, nastavenie monitorovania udalostí a implementovania potrebných technológií. Tieto kroky sú sumarizované pomocou diagramu aktivít.

Verifikácia metodiky prebehla v strednom podniku a na univerzite. Pri overení rámcovej metodiky boli stanovené základné bloky architektúry založenej na type klient-server. Bloky architektúry boli určené z hľadiska komunikácie medzi koncovým používateľom a serverom pri vykonaní požiadavky ukladania dát. Základným blokom sú *dáta* s ich vlastnosťami (pôvod, typ, klasifikácia, obsah). Dáta sú následne klasifikované a zaradené do druhého bloku *klasifikácie dát*. V metodike boli použité výlučne redundantné dáta, a preto tretí blokom je súbor *redundantných dát*. V ďalších krokoch architektúra zahŕňa požiadavky na koncového používateľa a server. *Správa kľúčov* je nastavením obmedzenia pre koncových používateľov. *Autorizačné úrovne* sú stanovené pre definovanie klienta a jeho operácií s dátami (zvýšenie bezpečnosti). *Šifrovací systém* je zvolený z uvedených teoretických východísk a výsledkov testovania, pričom sa nejedná o šifrovací systém, ale o hashovaciu funkciu.

Architektúru uzatvárajú komunikačné bezpečnostné protokoly *TLS a HTTPS*. Architektúra nezahŕňa nastavenie latencie, z dôvodu zbytočného obmedzenia.

V druhom kroku verifikácie bol vytvorený návrh infraštruktúry, ktorý vychádza z architektúry a splňuje odvodené bezpečnostné pravidlá. Pri návrhu architektúry boli zostavené dátové úložiská na základe uvedených komponentov s výberom podľa vzťahu výkon/cena/spotreba.

Tretí krok preverenia správnosti metodického rámcu bol prevedený inštalovaním virtualizačnej technológie KVM. Pre riešenie integrity dát bol využitý súborový systém ZFS.

Testovanie metodiky dokázalo, že navrhnutá metodika je správna, avšak niektoré zvolené technológie by bolo vhodnejšie riešiť iným výberom. K správne vybratým odporúčaniam bol priradený návrh architektúry, návrh infraštruktúry, hashovacia funkcia SHA, virtualizačné prostredie KVM. K doporučeniam na zváženie bol zaradený súborový systém ZFS z dôvodu jeho nestabilnosti pri nízkej kapacite veľkosti a hardvérová úprava v podobe zavedenia RAMdisku z dôvodu zníženia bezpečnosti.

4 Diskusia

Technológia cloud computingu sa stáva čoraz atraktívnejšou pre firmy. Vďaka jej škálovateľnosti a nákladom (platba iba za služby, ktoré využívame) je frekventovaná hlavne medzi veľkými a strednými podnikmi. Z ponúk služieb cloudu je najvyužívanejší modul SaaS (Software as a Service). Druhotný význam skratky modelu SaaS je ponuka služby ako úložiska dát (Storage as a Service), teda cloud ako virtuálne úložisko. Pokiaľ pristupujeme k modelu SaaS ako úložisku, tento modul sa stáva vhodným pre malé a stredné firmy. Podmienkou úspešnej implementácie v tomto chápaní je oddelenie povinností týkajúcich sa cloudu od firmy, a teda poskytovateľom cloudu sa stáva tretia osoba. Navrhovaným modelom a metodikou chcem dokázať efektívne využitie cloudu ako úložiska dát pre malé a stredné firmy s vlastným IT oddelením a hardvérom.

Cloud ako úložisko dát poskytuje zdieľanie (aj úpravy) rovnakých dát viacerým používateľom v reálnom čase. Táto vlastnosť je dôležitá pre vzdelávacie inštitúcie, ktoré vyžadujú aktuálne informácie a možnosť ich poskytnutia svojim zamestnancom a študentom. V záujme každej univerzity je ponuka nových informačných technológií so zameraním na aktuálne verzie softvéru a ich dostupnosť pre študentov. Túto vlastnosť dokáže plne pokryť cloudové prostredie, nakoľko aktualizácia aplikácií prebieha automaticky. Ďalšou výhodou, prečo by mal byť cloud využívaný v univerzitnom prostredí, je aktuálna disponibilita hardvéru univerzity a čiastočné odbúranie nákladov za platenie licenčných práv. Napriek uvedeným prednostiam je cloud v univerzitnom prostredí preferovaný iba na 4 percentá v rámci všetkých sektorov (najmenší podiel).

Hlavným negatívom cloudu či už v podnikovom alebo univerzitnom prostredí je bezpečnosť dát. Keďže dáta sú ukladané do virtualizovaného prostredia, predstavujú vyššie riziko odcudzenia zo strany tretej osoby, alebo aj samotného používateľa systému. Bezpečnosť je aktuálne posudzovaná na základe troch podmienok: utajenie, dostupnosť a integrita dát. Za najdôležitejšiu podmienku považujeme integritu dát, pretože iba na základe jej dodržania dokážeme poskytnúť relevantné dáta v akomkoľvek čase a na akomkoľvek mieste.

Prínos modelu a metodiky

Navrhovaný model predstavuje riešenie problému dát ukladaných do cloudu z hľadiska bezpečnosti dát. Model je zameraný na dve odlišné prostredia, a to univerzitu a podnik. Model je zameraný od nasadenia cloudu (riešenie hardvéru) až využitie cloudu ako úložiska s ohľadom na životný cyklus dát v danom prostredí.

Definovaná metodika poukazuje na riešenie kolíznych situácii pri implementácii cloudu ako úložiska dát s cieľom zvýšenia bezpečnosti ukladaných dát. Taktiež zahŕňa doposiaľ všetky možné riešenia bezpečnosti z pohľadu noriem, protokolov, metodík a algoritmov. Matematická formalizácia metodiky poskytuje nové hlbšie informácie o chovaní cloudu ako úložiska dát.

Diskusia s verejnosťou o navrhovanom riešení

Ohlasy na navrhovaný model a metodiku sú rozdelené do troch kategórií: čitatelia článkov, konferencie a stáž. Po publikovaní návrhu modelu v jazyku UML ma oslovili piati čitatelia. Ich otázky boli kladené prevažne na bližší popis modelu a ich návrhy môžem všeobecne zhrnúť ako požiadavky na špecifikovanie jednotlivých krokov modelu počas životného cyklu ukladaných dát. Nakoľko diagramy UML necharakterizujú postup veľmi podrobne, bolo by vhodné ich rozvinúť o bližšiu špecifikáciu, avšak je potrebné si uvedomiť do akej miery je vhodné diagramy rozširovať vzhľadom k ich výpovednej hodnote. Preto navrhujem nerozširovať celkový typ diagramu, ale iba jeho časť, a to zameranie na integritu dát prostredníctvom vytvorenia nových diagramov určených pre bližšiu charakteristiku menšieho celku hlavného diagramu.

Diskusie počas konferencií boli prevažne zamerané na riešenie rozdelenia koncových používateľov do bezpečnostných kategórií a rozdelenia dát podľa citlivosti. Zadelenie používateľa systému do určitej kategórie na základe právomoc je bežná situácia radenia používateľského účtu v systéme. Vytvorením kategórií a zoskupením používateľských účtov do kategórií bolo docielené rýchlejšie ovládanie a konfigurovanie používateľských účtov z hľadiska monitorovania udalostí (rizikové udalosti) a príslušným zmien vo firme a na univerzite. V tejto situácii je dôležité si uvedomiť do koľkých kategórií je potrebné účty rozdeliť a aké právomoci im prideliť. Uvedenú pripomienku je nutné vždy riešiť pre konkrétny podnik, alebo univerzitu a z nášho pohľadu je zovšeobecnenie prostredníctvom nášho modelu náhľadom pre základné možnosti aplikácie triedenia.

Ďalším významným postrehom získaným z konferencií bolo určenie významnosti modelu z hľadiska bezpečnosti. Doposiaľ nemôžem povedať do akej miery významnosti model patrí, nakoľko neboli doteraz publikované návrhy na delenie takýchto typov modelov. Napriek tomu, by bolo zaujímavé zadefinovať návrhy tried rozdelenia modelov zabezpečenia dát ukladaných do cloudu. Dané triedy by mohli byť klasifikované na základe použitia typu šifrovacieho systému, riešenia integrity dát, dostupnosti dát, ale aj na základe fyzického nasadenia na hardvér a softvérového riešenia modelu. V budúcnosti by som chcela svoj výskum zamerať na túto oblasť.

Počas stáže prebehlo niekoľko prezentácií navrhnutého modelu, pričom bol neustále vylepšovaný vzhľadom k pripomienkam z predchádzajúcej prednášky. Navrhnutý model ocenili experti z Moskovskej štátnej univerzity Lomonosova, ako aj Národnej ukrajinskej univerzity Tarasa Ševčenka v Kyjeve. Ich otázky poukazovali taktiež na zavedenie bližšieho popisu modelu a jeho možnej implementácie. Na základe vytvoreného diagramu balíčkov a diagramu tried sme sa uzhodli, že daný model nie je možné programovať z dôvodu jeho rozsahu a komplexnosti. Preto v práci bolo pristúpené k nasadeniu riešenia pomocou dostupných technológií.

Formalizácia Petriho siete pomocou matematických rovníc bola pre nich dôležitá, keďže vzhľadom k odstráneniu kritických situácií je najvhodnejšie využiť Petriho sieť a na základe jej matematického vyjadrenia je možné dokázať definovanie postupnosti krokov, ich ohodnotenie a celkový proces ukladania dát v cloude. Keďže

ide o zložitý problém (matica prechodu naznačuje vyššiu zložitosť v neskoršom rátaní s vektormi), bolo mi navrhnuté pre matematické vyjadrenie využívať MATLAB.

Z doposiaľ uvedených poznatkov z diskusií bol stanovený záver diskusie s verejnosťou. Model poskytuje nové možnosti riešenia bezpečnosti ukladaných dát v cloude vzhľadom na využitie aktuálne dostupného hardvéru a softvéru. Pre zvýšenie dôležitosti modelu je vhodné zadefinovať rozdelenie takýchto modelov do tried na základe bezpečnosti. Časť integritu dát je vhodné bližšie špecifikovať diagramami UML.

5 Záver

Bezpečnosť dát patrí k hlavným témam v informačných technológiách, nakoľko dáta sú považované za najcitlivejšie komponenty firmy. V súčasnej dobe je bezpečnosť dát zameraná na využitie novej technológie cloud computingu. Tento fakt vyplýva z nárastu využívania cloudu predovšetkým v podnikoch z dôvodu zníženia nákladov a urýchlenia správy informačných technológií.

K primárnym faktorom udržania bezpečnosti dát sú zavedené podnikové pravidlá. *Podnikové pravidlá* ovplyvňujú životný cyklus dát a práva koncových používateľov pri vykonávaní operácii s dátami. Forma týchto pravidiel býva interná nakoľko doposiaľ neboli stanovené všeobecné metriky a rámcové metódy pre zvýšenie bezpečnosti dát ukladaných v cloude.

Druhým významným faktorom je samotný *zamestnanec firmy*, ktorý s dátami pracuje. Pre zjednotenie práce zamestnancov pri vykonávaní ich funkcie sú odporúčané školenia s cieľom vysvetliť dôležitosť zabezpečenia dát a spôsoby bezpečnosti. Školenia by mali reagovať aj na rizikovú politiku podniku a pomôcť zamestnancom porozumieť identifikácii rizika a spôsobu jeho prevedenia.

Tretím krokom je monitorovanie udalostí a vytváranie auditov. *Monitorovanie udalostí* spravuje rizikové procedúry a identifikuje potenciálne hrozby ako zo strany klienta, tak zo strany serveru. Pravidelné vykonávanie *auditu* je prevedené za účelom identifikovania možných spôsobov odcudzenia a ich riešeniu. Audit vychádza z podnikových a bezpečnostných pravidiel, pričom jeho cieľom je hľadať nezabezpečené (slabo zabezpečené) miesta a na základe nich stanoviť nové smernice firmy.

Všeobecne sa rady pre bezpečnosť dát rozdeľujú na nízke (interné pravidlá) a vysoké (využitie DLP).

Hlavné ohrozenie dát vyplýva z nedostatočného utajenia dát, z dodržiavania integrity dát, ale aj z dostupnosti dát. Správne nasadenie cloudu do podnikového prostredia môže zvýšiť bezpečnosť firemných dát, nakoľko bezpečnosť dát by mala byť pre podnik hlavnou prioritou.

Cieľom tejto dizertačnej práce bolo navrhnúť metodiku zvýšenia bezpečnosti dát ukladaných do cloudu z pohľadu implementácie v podnikovom a univerzitnom prostredí. Bezpečnosť dát bola rozdelená do troch podmienok, a to utajenie, integrita a dostupnosť dát. Z literárnej rešerše vyplynula nekomplexnosť v riešení bezpečnosti v týchto odlišných prostredia. V súčasnosti existuje niekoľko protokolov, noriem, doporučení, pravidiel viazaných na zvýšenie bezpečnosti dát, avšak bez vzájomného prepojenia. Zameraním tejto práce bolo jasne stanoviť postupnosť krokov pri implementácii cloud computingu v podnikovom a univerzitnom prostredí so zvýšením bezpečnosti dát.

Navrhnutá rámcová metodika zhlukuje identifikované pravidlá obmedzenia voči koncovému používateľovi, šifrovaniu a bezpečnosti dát, identifikovaných rizík a integrity dát na základe teoretických východísk uvedených v práci a prevedeného testovania. Hlavný rozdiel medzi doposiaľ uvedenými metódami pre bezpečnosť dát a navrhnutou metodikou spočíva v komplexnosti návrhu so zameraním od inicializácie

cez stanovenie pravidiel až po samotnú arhcitektúru, infraštruktúru a virtualizačnú technológiu. Metodika je zostavená tak, aby ju bolo možné implementovať pre malé, stredné podniky a univerzity. Nasadenie tejto metodiky poskytuje stabilné a systémové riešenie bezpečnosti dát v implementovanom prostredí.

Pri verifikácii metodiky boli overované stanovené kroky na základe definovania blokov architektúry typu klient-server, návrhu infraštruktúry siete dátového centrálneho úložiska, zostavenia a úpravy hardvéru dátového úložiska, implementovania virtualizačnej technológie KVM a riešenia integrity dát pomocou súborového systému ZFS. Výsledky overenia potvrdili správnosť architektúry, infraštruktúry a virtualizačnej technológie s ohľadom na zníženie nákladov a nasadenie aj pre malý podnik. Prevedené úpravy hardvéru v podobe zavedenia RAMdisku ukázali, že nie je optimálnym riešením pre bezepčnosť dát, avšak jeho bezpečnosť je možné zvýšiť duplikáciou po sieti na ďalšie servery, alebo spomalenou synchronizáciou s SSD diskom. Testovaním súborového systému ZFS sa dokázalo, že pri dosiahnutí 95 percentnej a vyššej obsadenosti súborového systému sa stáva výkonnostný súborový systém takmer nepoužiteľným.

Prevedený prístup pri formalizácii rámcovej metodiky a jej následnej verifikácii umožnili splnenie základného cieľa práce a vytýčených krokov riešenia stanoveného problému bezpečnosti ukladaných dát v cloud computingu. Na základe uvedených faktov považujem cieľ práce za splnený.

6 Literatúra

Accenture. *A new era of sustainability. The global compact.* [online]. [cit. 2014-10-06] Dostupné z: http://www.accenture.com/sitecollectiondocuments/pdf/.

Ahson, S., Ilvas, M. *Cloud Computing and Software Services: Theory and Techniques.* New York: Auerbach Publications, 2011.

Ayad, A., Dippel, U. *Toward Virtual Machines High Availability: ZFS and Multi-Agent System.* New York: LAMP LAMBERT, 2011.

Barsoum, A. *Data Integrity in Cloud Computing Systems: Challenges and Solutions.* New York: LAMP LAMBERT, 2013.

Boneh, D., Franklin, M. K. *Identity-based encryption from the Weil pairing.* Londýn: Springer, 2001.

Boneh, D., Venkatesan, R. *Breaking RSA may not be equivalent to factoring.* Eurocrypt, 1998.

Cong, W., Sherman, S. M. Ch., Qian, W., Kui, R., Wenjing, L. *Privacy-Preserving Public Auditing for Secure Cloud Storage.* IEEE Trans.Computers, 2013.

Delic, K. A., Riley, J. A. *Enterprise Knowledge Clouds: Next Generation KM Systems?* Kankún: ICI, 2009.

Dittner, R., Rule, D. *Server Virtualization.* Burlington: Syngress Publishing, 2007.

Erikson, J. S., Spence, S., Rhodes, M., Banks, D., Rutherford, J., Simpson, E *Content-Centered Collaboration Spaces in the Cloud.* IEEE, 2009.

Erl, T., Puttini, R., Mahmood, Z. *Cloud Computing: Concepts, Technology Architecture.* New York: Prentice Hall, 2013.

Eswaran, A., Abburu, S. *Identifying Data Integrity in the Cloud Storage.* [online]. [cit. 2013-08-06] Dostupné z: http://ijcsi.org/papers/IJCSI-9-2-1-403-408.pdf.

Gartner *IT Glossary - defining in IT industry.* [online]. [cit. 2012-08-10] Dostupné z: http://www.gartner.com/it-glossary/cloud-computing/.

Gsoedl, J. *Hybrid clouds: Three routes to implementation.* [online]. [cit. 2012-12-12] Dostupné z: http://searchcloudstorage.techtarget.com/tip/Hybrid-clouds-Three-routes-to-implementation.

Hamilton, C. J. *Views of the solar system* [online]. [cit. 2012-05-10] Dostupné z: http://www.solarviews.com/eng/sun.htm .

Hanningan, I. *Data Handling Procedures in Government.* [online]. [cit. 2012-06-12] Dostupné z: http://www.cabinetoffice.gov.uk/sites/default/files/resources/datahandling-interim0.pdf.

Hayes, B. *Cloud computing.* ACM, 2008.

Hoff, Ch., Mogull, R., Balding, C. *Hacking Exposed: Virtualization and Cloud Computing: Secrets and Solutions.* New York: McGrawHill, 2013.

Henthorn, A. *Deploying Cloud Infrastructure at the Speed of the Cloud.* [online]. [cit. 2014-08-06] Dostupné z: http://www.datamation.com/cloud-computing/deploying-cloud-infrastructure-at-the-speed-of-the-cloud.html.

Hoppecke. *AquaGen premium.top.* [online]. [cit. 2012-11-05] Dostupné z: http://www.hoppecke.com/products/accessories/aquagenrpremiumtop.

Hugos, M., Hulitzky, D. *Business in the Cloud: What Every Business Needs to Know About Cloud Computing.* New York: John Wiley Sons, 2011.

Hurwitz, J. *Hybrid cloud for dummies.* New York: John Wiley Sons, 2013.

Český hydrometeorologický ústav *Informace ze stanice Brno-Žabovřesky..*

Chen, D., Zhao, H. *Data Security and Privacy Protection Issues in Cloud Computing.* International Conference on Computer Science and Electronics Engineering, 2012.

Iliaš, I., Guschlbauer-Hronek, K., Benesch, B., Bayer, G. *Slnko k službám: Možnosti využívania slnečnej energie.* Bratislava: Phare, 2006.

Juels, A., Kaliski, B. S. *Poors: proofs of retrievability for large files.* New York: ACM, 2007.

Kallahalla, M., Riedel, E., Swaminathan, R., Wang, Q., Fu, K. *Scalable secure file sharing on untrusted storage.* Berkeley: USENIX, 2003.

Klein, C., Kaefer, G. *From smart homes to smart cities: Opportunities and challenges from an industrial perspective.* Lecture Notes in Computer Science, 2008.

Kuyoro, S. O., Ibikunle, F., Awodele, O. *Cloud Computing Security Issues and Challenges.* International Journal of Computer Networks, 2011.

Leka, D. *Cloud Computing - The Glide OS Story: Solving The Cross Platform Puzzle.* New York: Happy About, 2013.

Lijun, M., Chan, W. K., Tse, T. H. *A tale of clouds: Paradigm comparisons and some thoughts on research issues.* IEEE, 2008.

Lim, I., Coolidge, E., Hourani, P. *Securing Cloud and Mobility: A Practitioner´s Guide.* New York: CRC Press, 2013.

Luhman, D. *Performance: Hyper-V vs. ESXi vs. KVM.* [online]. [cit. 2013-02-08] Dostupné z: http://luhman.org/blog/2012/05/01/performance-hyper-v-vs-esxi-vs-kvm-vs-virtualbox.

Martel, Ch., Nuckolls, G., Devanbu, P., Gertz, M., Kwong, A., Stubblebine, S. G. *A general model for authenticated data structures.* Algorithmica, 2001.

Marsh, Ch. *Data Integrity In The Cloud.* [online]. [cit. 2013-12-05] Dostupné z: http://www.wwpi.com/index.php?option=comcontentview=articlecatid=99:cover-storyid=12800:data-integrity-in-the-cloudItemid=2701018.

Mather, T., Kumaraswamy, S., Latif, S. *Cloud Security and Privacy.* New York: O´Reilly, 2009.

Mell, P., Grance, T. *Effectively and Securely Using the Cloud Computing Paradigm.* [online]. [cit. 2012-08-12] Dostupné z: http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt.

Mell, P., Grance, T. *The NIST Definition of Cloud Computing: Special Publication 800-145.* New York, 2011.

Microsoft. *SME role for cloud computing.* [online]. [cit. 2013-08-09] Dostupné z: http://www.microsoft.com/uk/smallbusiness/sbnews/growing-a-small-business/SME-role-forcloudcomputing-19227631.mspx.

Ming, L., Shucheng, Y., Kui, R., Wenjing, L., Thomas, H. *Toward privacy-assured and searchable cloud data storage services.* IEEE Network, 2013.

Nabil, S. *Cloud computing for education: A new dawn?* London: Elsevier, 2010.

Neha, T., Murthy, P.S. *A novel approach to data integrity proofs in cloud storage.* [online]. [cit. 2013-01-05] Dostupné z: http://www.ijarcsse.com/docs/papers/10October2012/Volume2issue10October.

Neosolar. *MultiPlus - uživatelská příručka.* 2008.

Neosolar. *Solárny panel IBC.* 2012.

Nielsen, L. *The Little Book of Cloud Computing SECURITY: 2013 Edition.* Rhode Island: New Street Communications, 2013.

Ning, C., Cong, W., Ming, L., Kui, R., Wenjing, L. *Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data.* IEEE Trans, 2014.

Pearson, S., Yee, G. *Privacy and Security for Cloud Computing.* Londýn: Springer, 2013.

Popa, R. A., Lorch, J. R., Molnar, D., Wang, H. J., Zhuang, L. *Enabling sexurity in cloud storage SLAs with cloudproof.* Berkley: USENIX, 2011.

Poynter, K. *Review of information security at HM Revenue and Customs.* Londýn: HM, 2008.

Praveena, K., Betsy, T. *Application of Cloud Computing in Academia.* Londýn: HM, 2000.

Priščáková, Z., Rábová, I. *Architecture, implementation, and security of cloud computing models.* Brno: Mendel University in Brno, 2012.

Priščáková, Z., Rábová, I. *An accessibility solution of Cloud Computing by solar energy.* Brno: Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 2013.

Priščáková, Z., Rábová, I. *Cloud v univerzitnom a podnikovom prostredí.* Karviná: Slezská univerzita v Opavě, 2013.

Priščáková, Z., Rábová, I. *Zvýšenie dostupnosti v Cloud Computingu.* [online]. [cit. 2013-12-05] Dostupné z: http://www.fem.uniag.sk/konferencieaseminare/zborniky/PriscakovaRabova.pdf.

Priščáková, Z. *Ako vybrať správny „oblak“ pre firmu.* [online]. [cit. 2013-10-12] Dostupné z: http://www.idbjournal.sk/rubriky/prehladove-clanky/ako-vybrat-spravny-oblak-pre-firmu.html?pageid=16222.

Priščáková, Z., Salák, J. *Hardware data store solution with greater data security.* Žilina: Publishing Institution of the University of Zilina, 2013.

Priščáková, Z., Rábová, I. *Model of data security for mid-range organizations with using the virtualized environments.* Košice: Technická univerzita v Košiciach, 2013.

Priščáková, Z., Rábová, I. *Model of solutions for data security in Cloud Computing.* Dilí: International Journal of Computer Science, Engineering and Information Technology, 2013.

Priščáková, Z., Rábová, I. *Solar Energy as a Primary Source of Energy for a Cloud Server.* Praha: Transactions on Electrical Engineering, 2013.

Priščáková, Z., Rábová, I., Salák, J. *The usage of cloud computing technology in university environment.* Brno: MENDELU, 2013.

Priščáková, Z., Salák, J. *Data Security for Cloud Storage Systems.* Žilina: Publishing Institution of the University of Zilina, 2014.

Priščáková, Z., Salák, J. *Levels of data categorization in cloud computing.* Hradec Králové: MAGNANIMITAS, 2014.

Priščáková, Z., Rábová, I. *The main aspects of data security in cloud computing.* New York: CPS, 2014.

Priščáková, Z. *Solution of the Cloud Computing Based on the System Response.* Brno: Mendel Univerzity in Brno, 2014.

Rhoton, J., Clercg, J., Graves, D. *Cloud Computing Protected.* New York: Recursive Press, 2013.

Rhoton, J., Haukioja, R. *Cloud Computing Architected.* New York: Recursive Press, 2013.

Rocha, F., Abreu, S., Correia, M. *The Next Frontier: Managing Data Confidentiality and Integrity in the Cloud.* IEEE, 2013.

Rouse, M. *What is private cloud (internal cloud or corporate cloud)?* [online]. [cit. 2012-08-08] Dostupné z: http://searchcloudcomputing.techtarget.com/definition/private-cloud.

Rouse, M. *What is public cloud?* [online]. [cit. 2012-08-08] Dostupné z: http://searchcloudcomputing.techtarget.com/definition/public-cloud.

Rouse, M. *What is hybrid cloud?* [online]. [cit. 2012-08-08] Dostupné z: http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud.

Ruest, D., Ruest, N. *Virtualizace - podrobný průvodce.* Praha: Computer Press, 2010.

Rybár, P. *Cloud computing – quo vadis?* [online]. [cit. 2012-08-10] Dostupné z: http://www.itnews.sk/tituly/infoware/2011-04-14/c139474-iw-cloud-computing-quo-vadis.

Sclater, N. *Cloudworks, eLearning in the Cloud.* [online]. [cit. 2013-06-09] Dostupné z: http://cloudworks.ac.uk/cloud/view/2430.

Sebe, F., Domingo-Ferrer, J., Martinez-Balleste, A., Deswarte, Y., Quisquate, J. J. *Efficient remote data possession checking in critical information infrastructures.* IEEE, 2008.

Singh, A., Liu, L. *A data sharing platform for outsourced enterprise storage environments.* IEEE, 2008.

Sosinsky, B. *Cloud Computing Bible.* New York: John Wiley and Sons, 2011.

Sravan, K. R., Saxena, A. *Data integrity proofs in cloud storage system.* IEEE, 2012.

Sullivan, D. *Hybrid cloud: It's not as secure as you think.* [online]. [cit. 2012-08-10] Dostupné z: http://searchcloudcomputing.techtarget.com/tip/Hybrid-cloud-Its-not-as-secure-as-you-think.

SUN. *Sun Cloud Architecture Introduction White Paper.* [online]. [cit. 2014-01-15] Dostupné z: http://developers.sun.com.cn/blog/functionalca/resource/cloudcomputing.pdf.

THURAISINGHAM, B. *Developing and Securing the Cloud.* New York: Auerbach Publications, 2013.

TUNCAY, E. *Effective use of cloud computing in educational institutions.* Procedia: Social and Behavioral Science, 2010.

VIRGINIA´S COMMUNITY COLLEGES. *Sensitive data definition.* [online]. [cit. 2012-05-12] Dostupné z: http://www.nvcc.edu/legal/sensitivedatadefinition.pdf.

VELTE, T., VELTE, A., ELSENPETER, R. *Cloud Computing, A Practical Approach.* New York: McGraw Hill, 2009.

VICTRON ENERGY. *BlueSolar charge controller MPPT 150/70.* [online]. [cit. 2012-11-12] Dostupné z: http://www.victronenergy.com/upload/documents/Datasheet20-20Blue20Sol0Charge20Controller20MPPT20150-7020-20rev200020-20EN.pdf.

WANG, Q., WANG, C., LI, J., REN, K., LOU, W. *Enabling public verifiability and data dynamics for storage security in cloud computing.* Berlín: Heidelberg, 2009.

WILLIAMS, M. *A Quick Start Guide to Cloud Computing: Moving Your Business into the Cloud.* New York: Kagan Page, 2010.

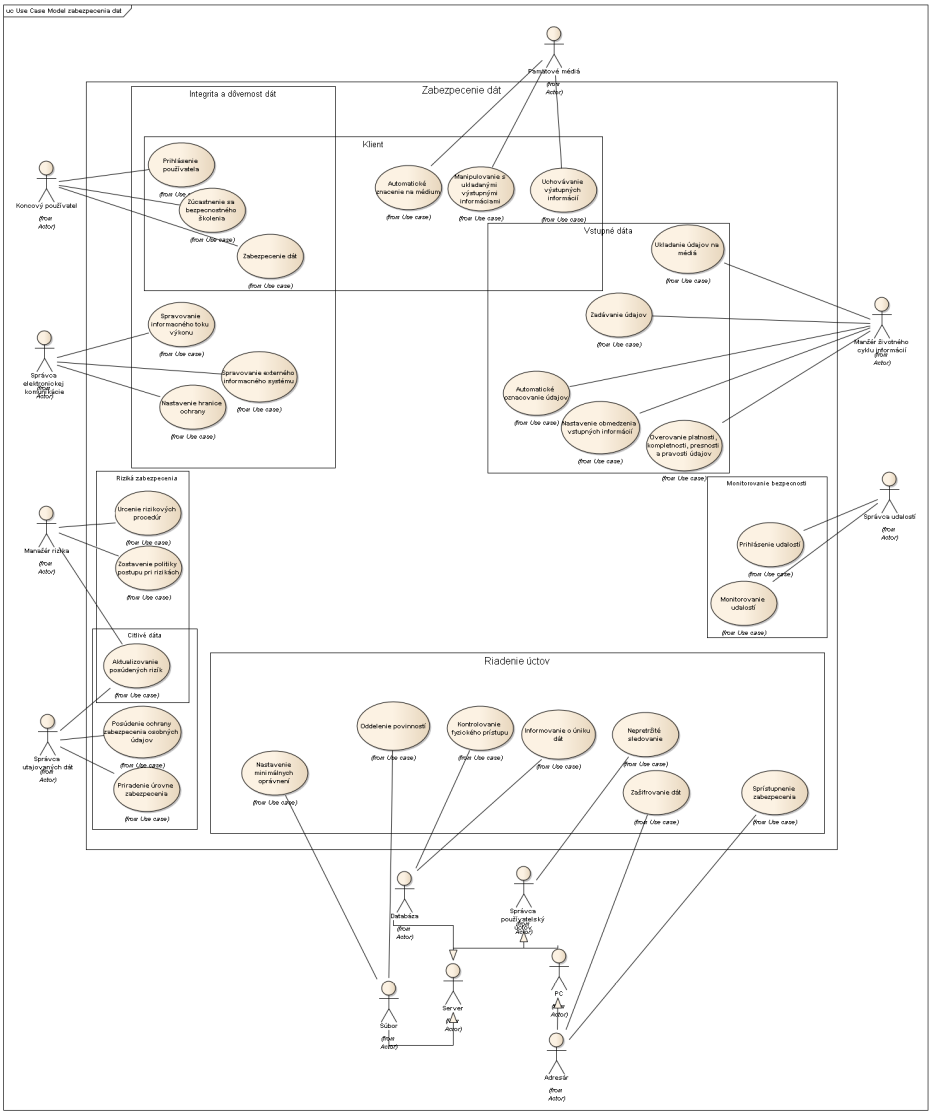
WINKLER, V. *Securing the Cloud.* New York: Syngress, 2011.

YANG, K. *Security for Cloud Storage Systems.* Londýn: Springer, 2014.

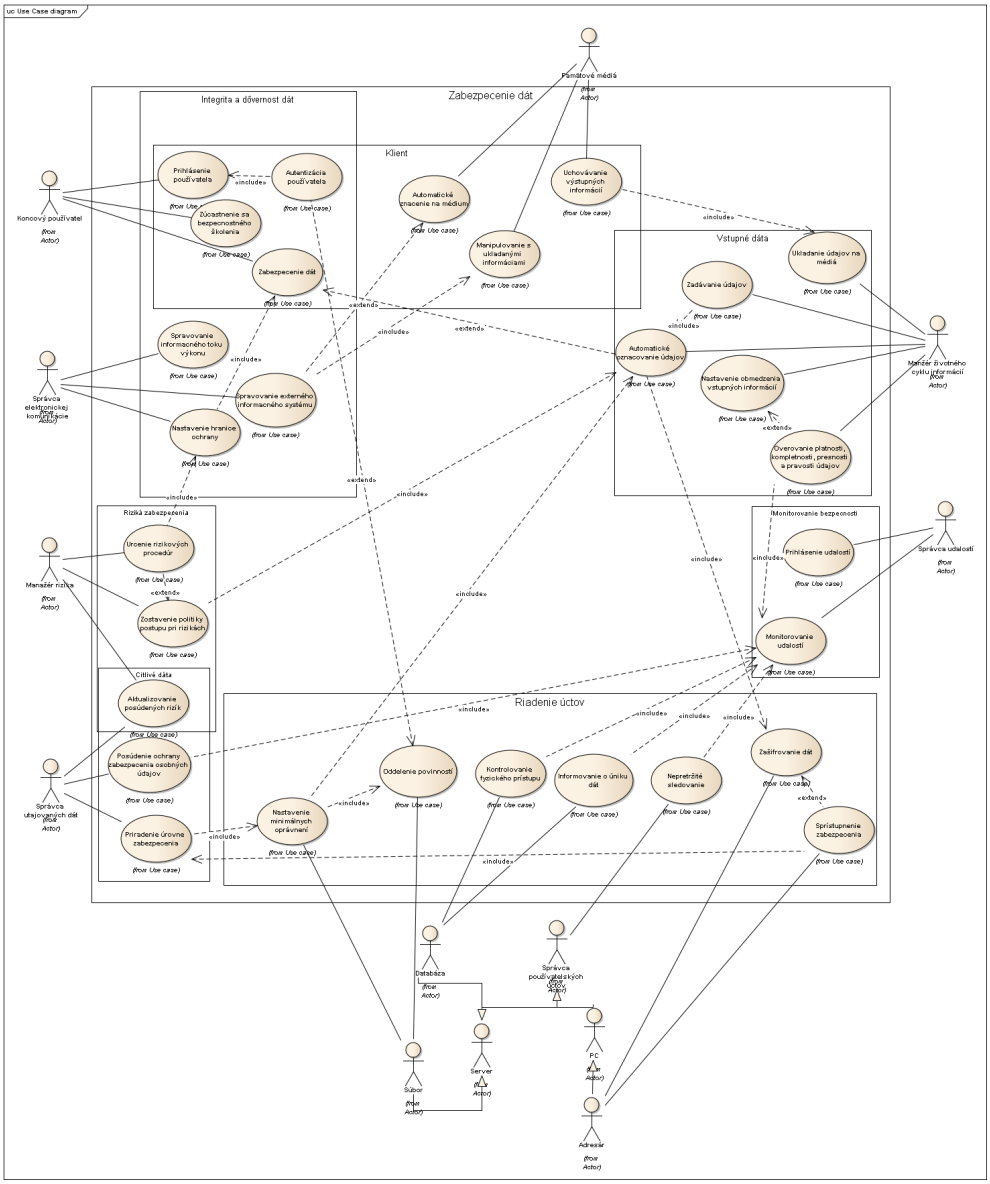
ZENG, K. *Publicly verifiable remote data integrity.* Berlín: Springer, 2008.

Přílohy

A Use case diagram modelu zvýšenia zabezpečenia dát ukladaných do cloudu



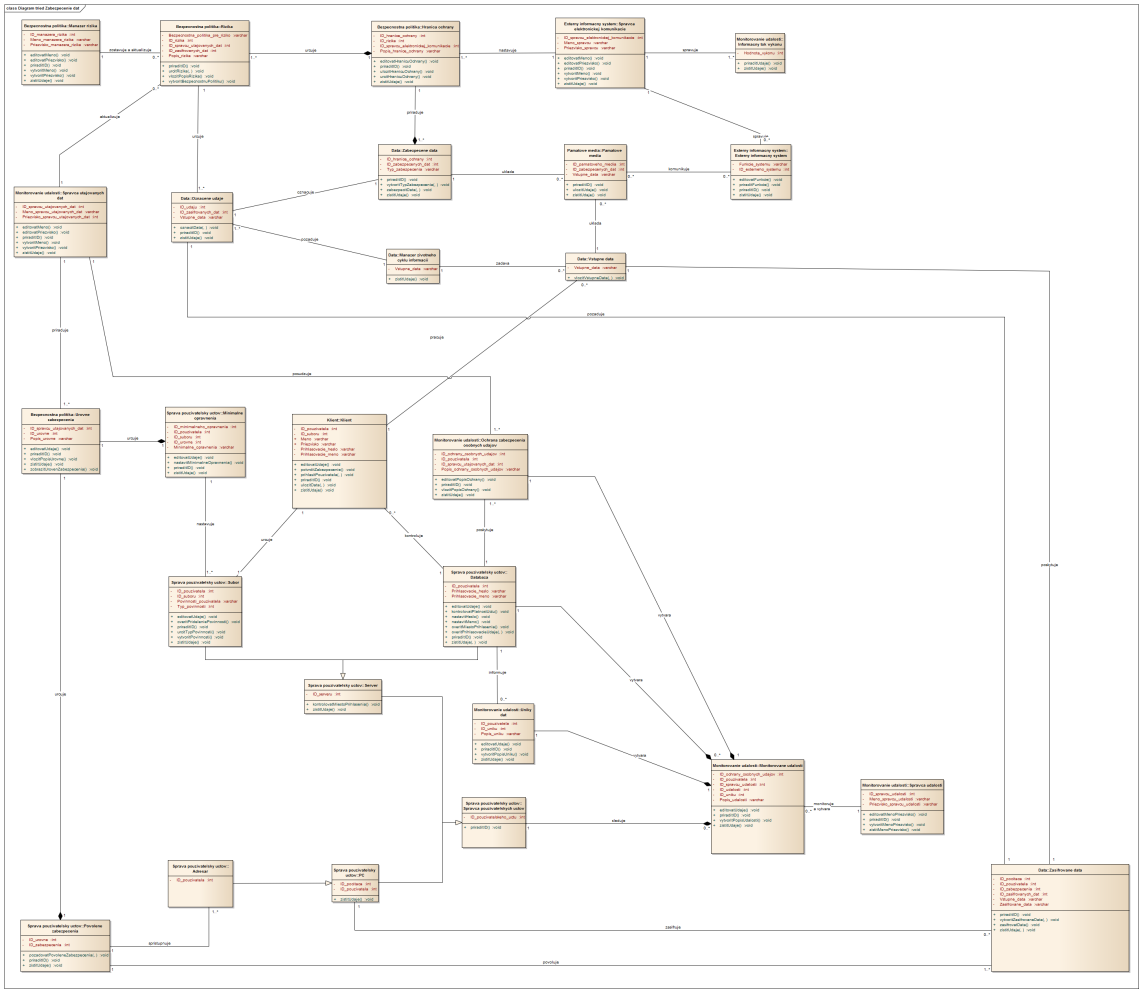
B Rozšírenie väzieb v use case diagrame



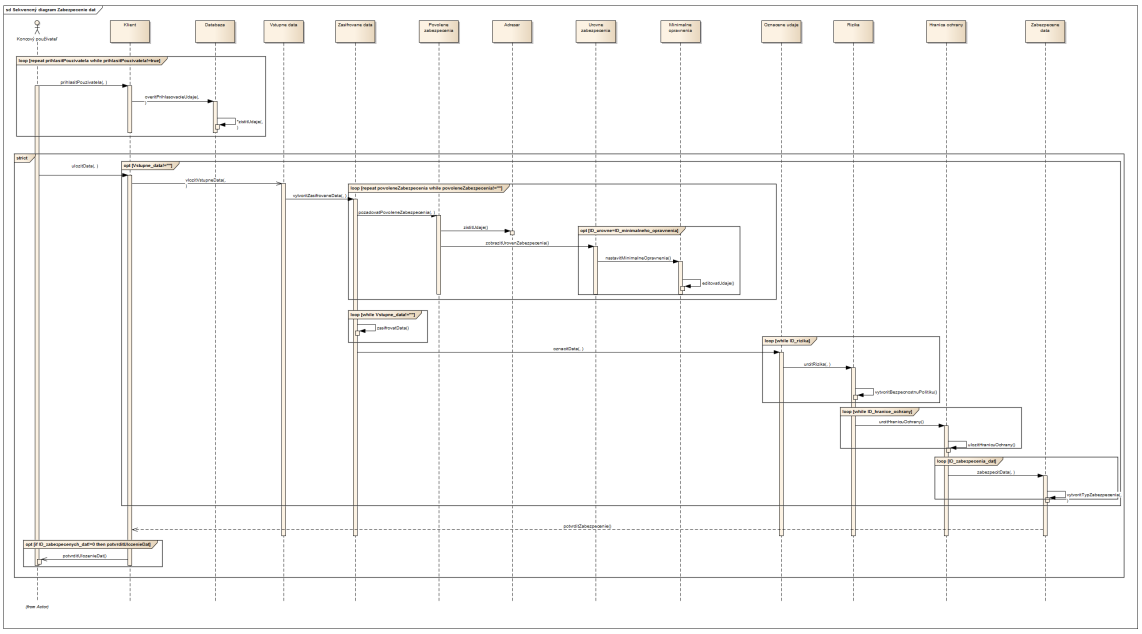
C Kontingenčná tabuľka vzájomných väzieb medzi prípadmi použitia, modulmi a aktérmi

Use case	Moduly						
	Citlivé dáta	Integrita a dôvernosť dát	Klient	Monitorovanie bezpečnosti	Riadenie účtov	Riziká zabezpečenia	Vstupné dáta
Aktualizovanie posúdených rizík	Správca utajovaných dát					Manžér rizika	
Autentizácia používatela		Koncový používateľ	Koncový používateľ				
Automatické oznacovanie údajov							Manažér životného cyklu informácií
Automatické znacenie na médium			Pamäťové médiá				
Informovanie o úniku dát					Správca používateľských účtov		
Kontrolovanie fyzického prístupu					Správca používateľských účtov		
Manipulovanie s ukladanými informáciami			Pamäťové médiá				
Monitorovanie udalostí				Správca udalostí			
Nastavenie hranice ochrany		Správca elektronickej komunikácie					
Nastavenie inimálních oprávnení					Správca používateľských účtov		
Nastavenie obmedzenia vstupných informácií							Manažér životného cyklu informácií
Nepretržité sledovanie					Správca používateľských účtov		
Oddelenie povinností					Správca používateľských účtov		
Overovanie platnosti, kompletnosti, presnosti a pravosti údajov							Manažér životného cyklu informácií
Posúdenie ochrany zabezpecenia osobných údajov	Správca utajovaných dát						
Prihlásenie používatela		Koncový používateľ	Koncový používateľ				
Prihlásenie udalostí				Správca udalostí			
Priradenie úrovne zabezpecenia	Správca utajovaných dát						
Spravovanie externého informacného systému		Správca elektronickej komunikácie					
Spravovanie informacného toku výkonu		Správca elektronickej komunikácie					
Sprístupnenie zabezpecenia					Správca používateľských účtov		
Uchovávanie výstupných informácií			Pamäťové médiá				
Ukladanie údajov na médiá							Manažér životného cyklu informácií
Urcenie rizikových procedúr						Manžér rizika	
Zabezpecenie dát		Koncový používateľ	Koncový používateľ				
Zadávanie údajov							Manažér životného cyklu informácií
Zašifrovanie dát					Správca používateľských účtov		
Zostavenie politiky postupu pri rizikách						Manžér rizika	
Zúcastnenie sa bezpecnostného školenia		Koncový používateľ	Koncový používateľ				

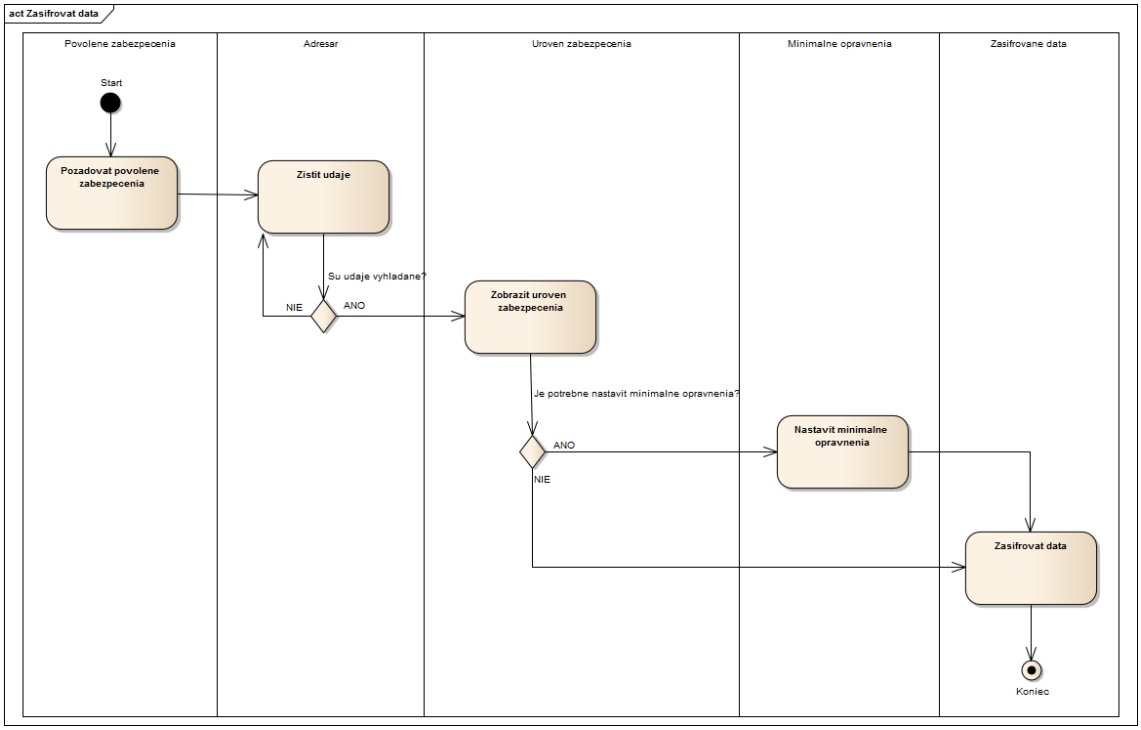
D Diagram tried modelu zvýšenia zabezpečenia dát ukladaných do cloudu



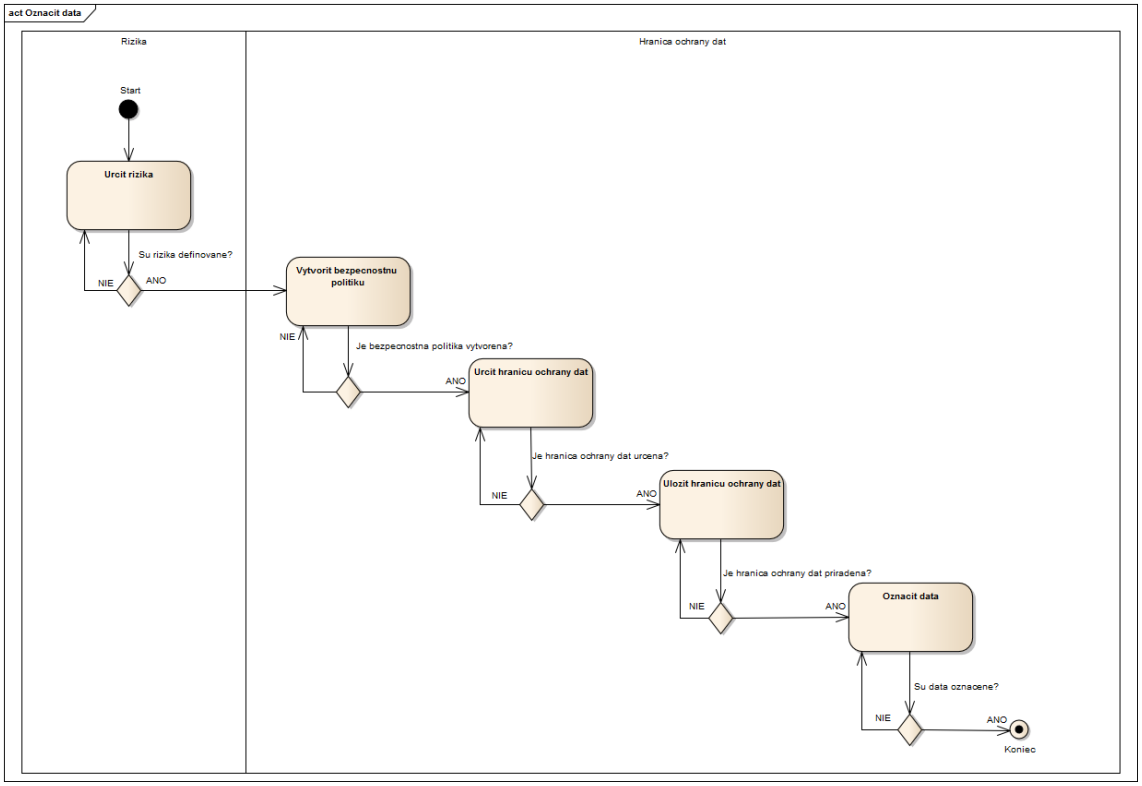
E Sekvenčný diagram modelu zvýšenia zabezpečenia dát ukladaných do cloudu



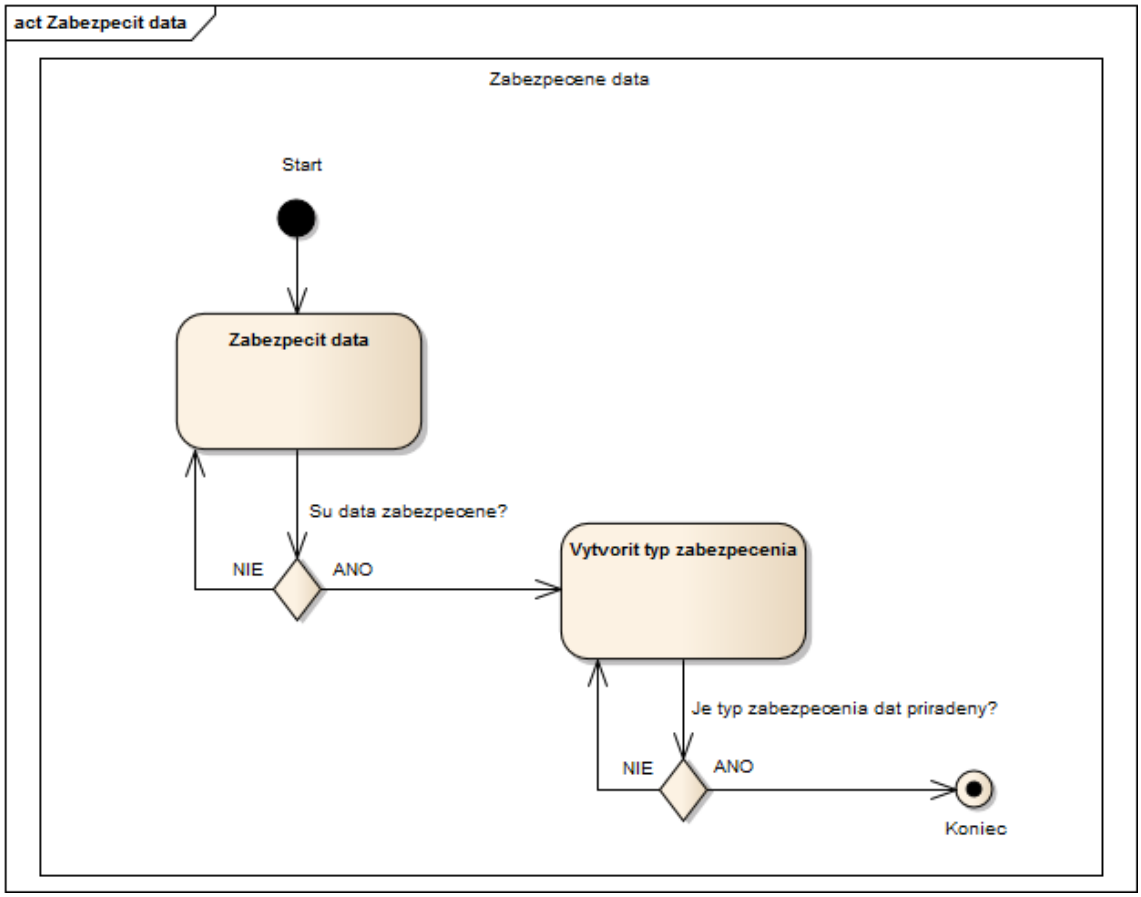
F Štrukturovaná aktivita Zasifrovat data



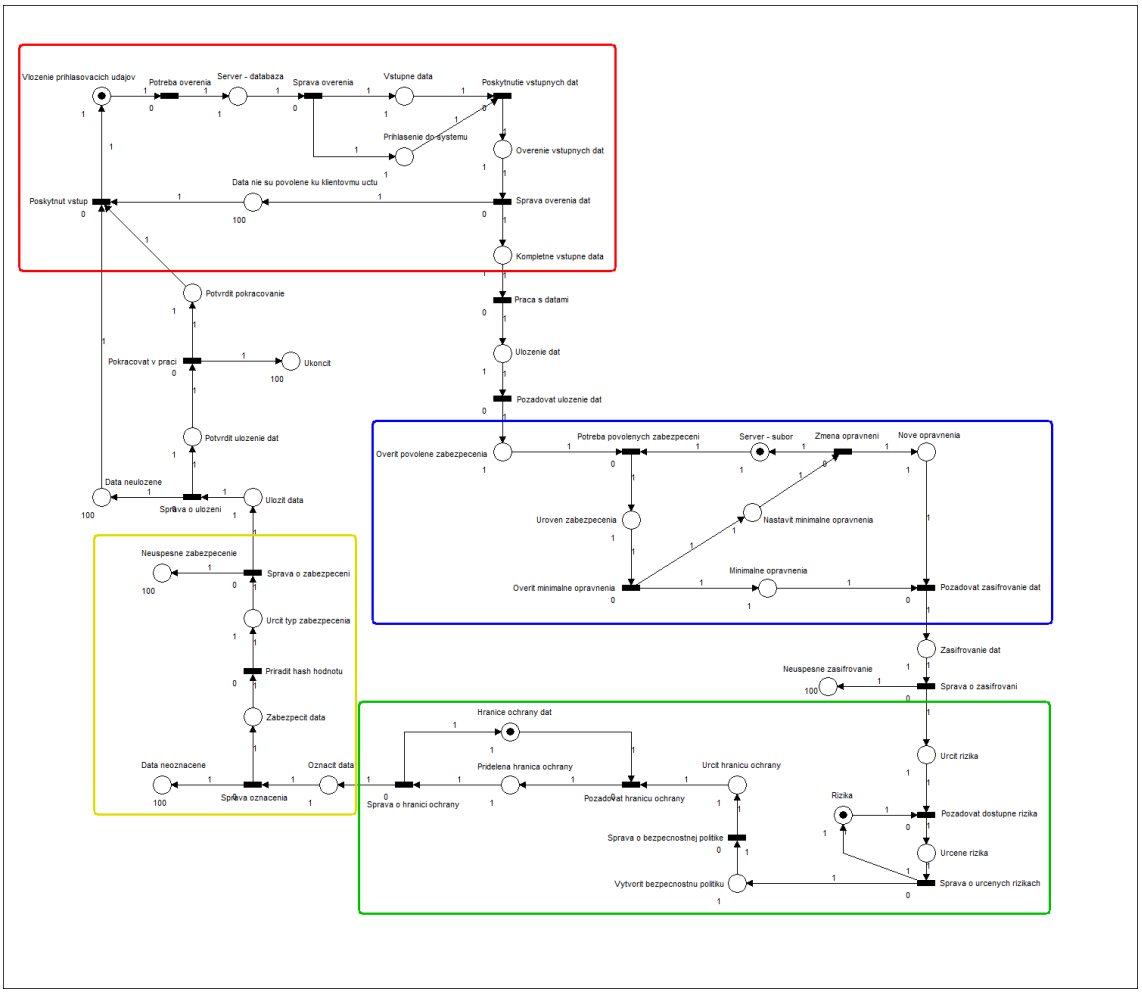
G Štrukturovaná aktivita Oznacit data



H Štrukturovaná aktivita Zabezpecit data



I Petriho sieť modelu zvýšenia zabezpečenia dát ukladaných do cloudu



J Konečný nedeterministický automat