UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

BAKALÁŘSKÁ PRÁCE

2017 Pavel Bárta

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Analýza zabezpečení cloud služeb

Pavel Bárta

Bakalářská práce

2017

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavel Bárta**
Osobní číslo:	**I14067**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Analýza zabepečení cloud služeb**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce bude provést analýzu a testování zabezpečení dat uložených ve veřejných cloud službách. Autor práce představí principy cloud služeb zaměřených na veřejný cloud, představí možnosti zabezpečení dat uložených v cloudu a provede jejich testování. Autor se zaměří na možnosti zabezpečení a šifrování dat v samotných cloud službách a zabezpečení dat pomocí nástrojů třetích stran.
V praktické části pak autor provede komparativní analýzu zabezpečení dat ve veřejných cloud jak pomocí interních i externích nástrojů.

Rozsah grafických prací:

Rozsah pracovní zprávy: **40 stran**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

ADAMS, Niall M. a Nicholas. HEARD. Data analysis for network cyber-security. London, UK: Imperial College Press, 2014. ISBN 9781783263745.

RAJANI, Sharma a Trivedi RAJENDER. Data Security in a Cloud Environment Using Multilevel Uec. 1. United States: LAP Lambert Academic Publishing, 2014. ISBN 9783659586958.

Vedoucí bakalářské práce: **Mgr. Josef Horálek, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2016**

Termín odevzdání bakalářské práce: **12. května 2017**

Univerzita Pardubice Česká republika

L.S.

Ing. Zdeněk Němec, Ph.D.
děkan

Mgr. Josef Horálek, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2017

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 11. 5. 2017

Pavel Bárta

PODĚKOVÁNÍ

Chtěl bych zde poděkovat Mgr. Josefu Horálkovi Ph.D., za pomoc a cenné rady při zpracování bakalářské práce.

ANOTACE

Úvodní část práce seznamuje čtenáře s definicí cloud computingu, včetně možností jeho využití. Následuje představení a popis základních charakteristik a principů, včetně několika druhů modelů, které definují druh cloudu, a poté srovnání výhod, či nevýhod cloud computingu. Další podstatnou částí je představení jednotlivých cloudových úložišť, které nynější poskytovatelé nabízí a jejich charakteristik. Práce pokračuje úvodem do základního šifrování a představením nástrojů, které umožňují šifrování dat před uložením v cloudu. V praktické části jsou uvedeny výsledky měření zatížení systémových prostředků těmito nástroji.

KLÍČOVÁ SLOVA

cloud, úložiště, šifrování, zabezpečení, nástroje,

TITLE

Security analysis of cloud services

ANNOTATION

The introductory part of the thesis introduces the reader to the definition of cloud computing, including the possibilities of its use. The following section contains introductions and descriptions of basic features and principles, including several types of cloud defining models, and then comparing the advantages and disadvantages of cloud computing. The following is the presentation of the individual cloud repositories that the current providers offer and their characteristics. Thesis continues by introducing basic encryption and introducing tools that enable data encryption before sending to the cloud. The practical part shows the results of measuring the load of system resources using these tools.

KEYWORDS

cloud, storage, encryption, security, tools

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK

AES – Advanced Encryption Standard

CBC – Cipher Block Chaining

FTP – File Transfer Protocol

HMAC – Hash-based Message Authentication Code

HTML – HyperText Markup Language

IM – Instant Messaging

IT – Information Technology

MIT – Massachusetts Institute of Technology

NIST – National Institute of Standards and Technology

OAEP – Optimal Asymmetric Encryption Padding

PBKDF2 – Password-Based Key Derivation Function 2

PKCS – Public Key Cryptography Standards

RSA –Rivest, Shamir, Adleman

SHA – Secure Hash Algorithms

SMB – Server Message Block

SSL – Secure Sockets Layer

TLS – Transport Layer Security

VPS – Virtual Private Server

ÚVOD

Cloud computing lze chápat jako stále se více rozšiřující princip provozování široké škály služeb nebo programů, který přímo využívá služeb internetu. Na trhu lze najít velké množství oblastí a odvětví, kde se služeb „cloudu“ využívá. Příklady cloud computingu mohou být například: virtualizace serverů, síťové nástroje, databázové služby a samozřejmě také virtuální úložný prostor. Existují placené i volné varianty poskytování výše uvedených služeb a různé způsoby, jakými jsou poskytovány. V aktuální době se lze stále častěji setkat s případy přečtení a krádeže dat třetí stranou, a tudíž je nutno implementovat některá z bezpečnostních opatření sloužících k ochraně proti neautorizovanému přístupu a přečtení dat.

Cílem bakalářské práce je analýza a testování možností zabezpečení služeb cloudu se zaměřením na uložená data ve veřejném cloudu, včetně porovnání samotných produktů s jejich možnostmi a parametry.

V teoretické části proběhne nejdříve definice a obecné představení principů cloudu, jejich parametrů, možností dělení a charakteristik. Následovat bude zaměření na datová úložiště, kde budou specifikovány parametry, aktuální poskytovatelé a alternativy dostupnosti pro klienta. V neposlední řadě bude provedena analýza nabídky cloudových úložišť, a to jak volných, tak i placených s důrazem na podmínky využívání, cenu, a poskytované zabezpečení dat. Dalším krokem bude obecná definice a vysvětlení šifrování, po kterém bude následovat zaměření na šifrování dat v cloudu, kde proběhne rozdělení možností zabezpečení na straně uživatele a serveru.

Předmětem praktické části bude srovnávací analýza možností zabezpečení dat ve veřejných cloudových službách. Zkoumány a testovány budou převážně externí nástroje s různou velikostí a množstvím zkoumaných datových vzorků. Sledovány budou požadavky na prostředky klienta a doba provádění, což jsou parametry nutné pro efektivní a objektivní vyhodnocení a porovnání daných nástrojů.

V práci bude využita podstatná část terminologie v cizím jazyce, přičemž bude její první výskyt uveden v závorce česky.

1 CLOUD (CLOUD COMPUTING)

1.1 Definice

Informace v následující kapitole vychází z informací, které byly čerpány z [6] a [31]

Cloud computing (cloud) nemá žádnou, jednotně standardizovanou definici. Platí zde však určitá fakta a principy, které platí ve všech oblastech, do kterých činnost a funkcionality cloudu zasahují, a které ovlivňují. Základním stavebním kamenem je kombinace služeb virtualizace s technologií WEB, která zajišťuje prostředky pro širokou škálu dynamicky poskytovaných, elektronických služeb. Tyto služby by měly být dostupné jednak na základě konkrétního požadavku, nebo kdykoliv podle potřeby, v závislosti na druhu a rozsahu využívané služby. Jak již bylo řečeno, neexistuje žádná unifikovaná definice cloudu, avšak jednou velmi často zmiňovanou a nadále využitou je rozdělení na pět základních charakteristických rysů, tři různé servisní modely a pět odlišných modelů nasazení. Tuto definici stanovila organizace NIST. Definice bude nadále popisována a rozebírána [6].

1.2 Možnosti využití

Cloud se od počátku své historie, která bude dále stručně představena, rozrostl do takových rozměrů, že momentálně zasahuje téměř do všech oblastí lidského života, i když o tom běžní uživatelé internetu ani nevědí. V tomto oddíle budou stručně popsány některé z možností využití cloud computingu, avšak se tato práce bude zaměřovat převážně na cloudová datová úložiště.

Email

Jednou z nejrozšířenějších odvětví cloudu je jednoznačně využívání emailových služeb. Denně projdou internetem astronomická množství emailových zpráv, a tak není pochyb o možnostech, které cloud v souvislosti s elektronickou poštou nabízí.

Virtuální privátní server (VPS)

Dalším, velmi rozšířeným odvětvím, je virtualizace serverů. Firmy s cílem ušetřit finance, prostor a čas, při správě serveru na vlastním hardware (HW), implementují do svého systému již hotová serverová řešení, která jsou poskytována pro širokou škálu využití a s různými funkcionalitami. Řadíme zde virtualizaci veškerých serverových služeb.

Obecné uživatelské aplikace

Na trhu jsou taktéž k dispozici různé druhy běžných uživatelských aplikací, mezi které patří téměř cokoliv, co běžný uživatel na svém elektronickém zařízení využívá. Řadí se sem kancelářské nástroje, grafické editory a v neposlední řadě jsou jistým druhem cloudu také sociální sítě, včetně početných portálů pro sledování videa. Můžeme sem ještě zařadit různé druhy komerčního SW (software), v podobě ekonomických nástrojů, informačních systémů a systémů pro řízení.

Cloud networking

Virtualizace síťově infrastruktury se s rozmachem cloudu stává velice moderním pohledem na pojetí počítačových sítí. Můžeme virtualizovat například: routery (směrovače), firewally, přenosové pásmo a různý SW určený pro správu sítě [60].

Datová úložiště

Využití cloudu, jako datového úložiště, úzce koresponduje se všemi výše zmíněnými oblastmi a mnohými dalšími. Jedná se o nejvíce rozšířené odvětví cloud computingu, které usnadňuje práci a šetří prostředky vzhledem k absenci nutnosti vlastnictví HW, a s tím související správou a personálním zajištěním. Tato práce bude dále zaměřena právě na cloud computing v souvislosti s datovými úložišti a veškeré detailní informace, principy a možnosti budou uvedený dále.

1.3 Historie

Ač slova „cloud computing“ mohou působit, jako velmi mladý a moderní pojem, tak bude překvapením, že první zmínka o prapočátku teorie cloudu je řečena počátkem 60. let 20. století, kdy John McCarthy, profesor působící na univerzitě MIT přirovnal sdílení počítačových prostředků a souvisejících technologií ke sdílení elektrické energie. Podobnost spočívá v myšlence, že bez elektřiny se neobejde řada domácností nebo společností, protože mají zakoupena zařízení, které ji čerpají, avšak nikdo si z tohoto důvodu nepostaví vlastní zdroj energie, jako je například elektrárna. Mnohem logičtější je centrální elektrárna, na kterou je připojeno velké množství uživatelů a jsou na ni napojeni na dálku pomocí rozvodné soustavy. Tato myšlenka je mnohem složitější a hlubší, přičemž zasahuje i do oblasti virtualizace (v této době ještě neexistující), protože neexistuje pouze jedna elektrárna, ale je jich více, a ty jsou navzájem spojené. V případě poruchy některé z nich nebo při přerušení spoje vedoucího k ní, ostatní elektrárny přebírají její zodpovědnost a pokrývají i její oblast působení.

Koncového spotřebitele se to nijak netýká, protože s případným malým záchvěvem nepocítí změnu činnosti na svém zařízení. Analogicky k sobě můžeme přirovnat elektrárny s datovým centrem, rozvodnou soustavu s internetem, a uživatelský spotřebič s koncovým zařízením [33].

2 PRINCIPY (ATRIBUTY) CLOUDU

S vývojem informačních technologií rostou také možnosti a varianty poskytování cloudových služeb. Dle požadavků a předpokládaného rozsahu využití je možné zvolit optimální druh služeb pro daný účel s ohledem na finanční náročnost zvolené varianty, a pokrýt tak široké spektrum činností, které mohou být implementací některého z cloudových řešení výrazně zjednodušeny.

2.1 Základní charakteristiky

Běžně se uvádí pět nebo šest různých základních charakteristik. Tyto rozdíly jsou způsobeny právě absenci jednotné standardizované definice cloudu, a tak bude uvedena verze obsahující právě šest vybraných základních principů. Celá podkapitola je založena na informacích získaných ze zdroje [19].

Orientace na služby

Aby měl cloud computing vůbec nějaký význam a účel, musí uživateli něco poskytovat, něco nabízet. V tomto případě bude předmětem poskytování nějaká služba, nebo skupina určitých služeb a produktů. Jak již bylo výše popsáno, prostřednictvím cloudu je možno využívat skutečně široké spektrum služeb cílených jak na koncové uživatele, tak i na větší subjekty.

Škálovatelnost a elasticita

Tyto pojmy souhrnně říkají, že by se funkčnost výše zmíněných nabízených služeb měla přizpůsobit aktuálním požadavkům a potřebám koncového uživatele. Toto přizpůsobení platí samozřejmě v rámci možného maximálního výkonu a systémových prostředků poskytovatele služby, a samozřejmě také na velikosti rozsahu zakoupené funkcionality. (v případě zpoplatněných služeb)

Sdílení informací

Jak již z podstaty cloud computingu plyne, data, s kterými aplikace a služby pracují, jsou uložena někde „v cloudu“. Díky této myšlence je velmi snadné zpřístupnit dané informace v reálném čase komukoliv, kdo s nimi má právo a možnost pracovat nezávisle na tom, kde se právě nachází a kolik uživatelů s daty chce pracovat. Cílem této myšlenky je umožnění práce s daty více uživatelům v jeden okamžik a umožnit jim vzájemnou kooperaci. Samozřejmostí je nutnost internetového připojení pro přístup ke vzdáleným prostředkům.

Poplatek za užívání

Existují jak varianty služeb, které jsou poskytovány zcela zdarma, tak i alternativy, za které je nutno poskytovateli zaplatit určitý obnos. V závislosti na druhu poskytované služby mohou být účtovány poplatky rozdílným způsobem. Příkladem může být částka účtovaná za jednotku času, výpočetního výkonu, či objemu dat.

Zaměření na výsledek

Tento princip říká, že poskytované služby a funkcionality by měly být stavěny tak, aby poskytovaly co nejlepší výsledek, který koncový uživatel očekává (intuitivní a jednoduché ovládací rozhraní, efektivní vykonávání zadaných činností a ideálně co nejnižší složitost případné implementaci či údržby). Z praktických zkušeností a historických údajů je zřejmé, že se z těchto šesti principů jedná o ten nejvíce problémový.

Využití internetu

Vzhledem k samotnému konceptu cloud computingu, nelze bez využití internetu cloud jako takový využívat. Jedná se totiž o jedinečnou, globálně rozšířenou a standardizovanou technologii (síť) pro přenos dat.

2.2 Distribuční (servisní) modely

Poskytování služeb cloud computingu je rozděleno do tří distribučních modelů, které vypovídají o tom, jakým způsobem jsou služby cloudu poskytovány. Představení poskytovatelů každého, z níže uvedených modelů, bude předmětem práce později. Významným zdrojem informací této podkapitoly je [43].

Infrastructure as a Service (IaaS)

Jak již z názvu plyne, podstatou tohoto modelu je pronájem kompletní cloudové infrastruktury. Zahrnuje pronájem serverových produktů, systémů pro zálohu dat, datových úložišť, a také různých síťových prostředků, jako třeba firewallu.

Služby jsou k dispozici ihned po případném zaplacení a disponují možností plynulé změny jejich parametrů. Dnes známe model IaaS jako poskytování hostingových služeb virtuálních datových úložišť.

Výhodou je bezesporu možnost, že koncovému uživateli odpadá nutnost zajištění správy a údržby HW, na kterém jsou služby provozovány. Tato povinnost přechází na poskytovatele, který přebírá zodpovědnost za jeho správný chod a údržbu. Nevýhodou zde může být fakt, že naše data, včetně případných citlivých, jsou uložena na obvykle fyzicky nedostupném místě, a tak nad nimi zákazník nemá plnou kontrolu.

Platform as a Service (PaaS)

PaaS je dalším distribučním modelem cloud computingu. Slovo platforma má v tomto případě význam kompletního aplikačního nebo vývojového prostředí (nebo obou současně). Koncept PaaS lze pozorovat ze dvou úhlů.

Prvním je možnost pronájmu vývojářům, kterým bude služba sloužit pro vývoj aplikací. Druhým je pronájem služeb větším společnostem, jejichž správa IT na pronajaté platformě vyvine aplikaci, která slouží jejich zaměstnancům. V obou těchto případech je výsledný vyvinutý produkt dále provozován a poskytován jako SaaS služba.

Software as a Service (SaaS)

Model SaaS byl již nepřímo zmíněn při popisu možných služeb, které cloud nabízí. Významnými zástupci jsou webmailoví klienti, kterých je na trhu celá řada. Dalším je IM, který však již postupně přechází do oblasti sociálních sítí, které se do oblasti významu tohoto modelu částečně řadí taktéž.

Tento model zahrnuje SW, který je provozován jak na straně serveru, tak i klienta. SW obou stran je provozován na infrastruktuře poskytovatele služby. K využití je potřebná instalace konkrétní aplikace, případně webového prohlížeče. Výhodou možnosti použití prohlížeče je nezávislé použití na různých operačních systémech, a to i mobilních. V současné době probíhá zdokonalování nabídky produktů využívajících tuto platformu, a přibývají aplikace zabývající se kancelářským SW a antivirovými řešeními.

Ostatní

Dalšími, avšak méně rozšířenými modely jsou BaaS (Backup as a Service), MaaS (Monitoring as a Service), anebo třeba CaaS (Communication as a Service) [16].

2.3 Modely nasazení

Tento způsob klasifikace nám říká jakým způsobem, a s jakým druhem přístupu je cloud poskytován v kombinaci s danou službou. Zdroje informací nutné k výstavbě této podkapitoly byly hlavně [15], [33] a [43].

Public cloud (veřejný cloud)

Model, který zahrnuje produkty, nabízené uživatelům z řad široké veřejnosti. Obvykle jsou služby poskytovány z vlastních sdílených prostředků poskytovatele. Bývá určen téměř neomezenému rozsahu uživatelů, případně nějakému většímu množství zákazníků, kteří službu využívají buď zdarma, případně za nějaký malý poplatek, při zachování téměř stejných možností pro všechny uživatele. Dále může být zaměňován s outsorcingem, ale musí splňovat všechny charakteristiky cloud computingu. Zástupci takových cloudů jsou Skype či Seznam.cz

Private cloud (soukromý cloud)

Rozsah působnosti poskytovaných služeb tohoto typu cloudu je pouze v rámci uzavřené organizace (firmy, sdružení apod.). Slouží pouze k internímu využití členy dané organizace a je vytvářen a provozován obvykle samotnou organizací či společností, případně externím poskytovatelem služeb tohoto typu.

Hybrid cloud (hybridní cloud)

Hybridní cloud vzniká kombinací veřejných a privátních variant cloudových služeb. Pro uživatele se vše jeví, jako kdyby pracoval na jednom druhu cloudu (privátním), avšak se jedná o interní propojení obou zmíněných modelů. Obvykle jde o kombinací privátního cloudu vlastněném určitou organizací, s externími službami dalšího poskytovatele.

Community cloud (komunitní cloud)

Tento model je často tvořen spojením prostředků tzv. komunity (skupiny členů, kterou seskupuje určitá společná vlastnost). Prostředí je pod správou a vlastnictvím dané komunity, a stejně tak je poskytováno určené skupině uživatelů.

2.4 Výhody a nevýhody využívání cloud computingu

Ač je využívání cloudu v dnešní době trendem, a stále více se rozšiřuje jak na úrovni firemní, tak i v případě běžného uživatelského použití, nemusí nutně být vždy ideálním řešením. V následující části práce budou shrnutý výhody a nevýhody nasazení a implementace využití cloudových služeb.

Je nutné stanovit dva pohledy hodnocení. Hledisky, na kterých budeme posuzovat případnou výhodnost, jsou technické aspekty a finanční aspekty.

Finanční aspekt

V případě využití cloudu jsou počáteční investice obvykle velmi nízké, protože zařízení, na kterých bude cloud provozován, je v závislosti na použitém modelu cloudu spravován poskytovatelem služeb. Jedinou případnou, doplňující investicí, by měla být modernizace internetové a lokální konektivity pro zajištění plynulého chodu všech pořízených služeb.

V případě provozování systému, se službami na vlastním HW, je v mnoha případech nutná rozsáhla pořizovací investice do kompletní infrastruktury a jako více než pravděpodobný se jeví příchod dalších investic, které souvisejí s chodem zařízení. Samozřejmostí je nutnost personálního obsazení správci systémů [33].

Technický aspekt

Při využití cloudu existuje obvykle možnost velmi rychlého pořízení služeb a samotného zavedení do chodu. Uživateli odpadá takřka veškerá nutnost správy HW, a často i SW, o kterou se stará provozovatel. Stejně tak je zde jednoduché dynamické rozšiřování druhu poskytovaných služeb, zvyšování výkonu, a zavádění nových modulů. Nevýhodou zde může být pomyslná absence kontroly nad HW, na kterých jsou uložena data uživatele, ale v praxi jsou stále častěji zaváděny mechanismy zabraňující zneužití dat třetí stranou.

Jak již bylo naznačeno, v případě provozu systému na vlastní infrastruktuře přibývá nutnost rozšíření personálního obsazení obsluhy a údržby systémů. S tím souvisí nutnost specifických odborných znalostí a další investice do vzdělávání. Velkou výhodou zde však je fakt, že uživatel je zároveň provozovatelem cloudu se vším, co k tomu náleží a má veškerý HW a SW pod svojí kontrolou. V případě, že proběhne dostatečně velká investice do infrastruktury, je možnost stát se zároveň poskytovatelem, a určité služby nabízet dalším uživatelům [33].

2.5 Některé další důležité pojmy a vlastnosti

Základní informace o definicích následujících pojmů byly získány ze zdroje [15].

Multi-tenancy

Z principu fungování cloudu je obvyklé, že danou službu, prostředek či zařízení využívá více než jeden uživatel, aniž by každý z nich věděl o ostatních (Výjimku tvoří služby určené právě pro kooperaci více uživatelů apod.). Princip multi-tenancy zajišťuje oddělení jednotlivých uživatelů, aby žádný z nich nemohl zasahovat do služeb či výpočetního prostředí kohokoliv dalšího.

Tenants in control (Správa nájemníků)

Pojem souvisí s výše zmíněným principem multi-tenancy. V tomto případě je možnost každého koncového zákazníka (uživatele), upravovat si libovolně s ohledem na omezení daného systému parametry, výpočetní výkon, nebo druh poskytovaných služeb, a to vše bez nutnosti zásahu odpovědné osoby, obvykle správce nebo přímo poskytovatele. Takovéto změny mohou být, a obvykle jsou zpoplatněny v závislosti na nastavených službách a parametrech.

Federace (Federation)

Federace vzniká sloučením několika individuálních prostředků. Takovýto výsledný produkt navenek působí jako jeden rozsáhlejší a lze s ním tak i zacházet. Produktem (službou) jsou v tomto případě balíčky, jejichž parametry jsou odlišné kvalitou a kvantitou obsažených funkcionalit.

Fond prostředků (Resource pooling)

Fond vznikne sloučením několika různých prostředků v tom smyslu, aby je bylo možné nabízet za požadovaných podmínek s určitou úrovní kvality a kvantity.

3 CLOUDOVÁ ÚLOŽIŠTĚ

Jak již bylo výše uvedeno, cloudová úložiště tvoří podstatnou část služeb cloud computingu. Potřeba sdílení dat v reálném čase narůstá a podmínka nepřetržitého přístupu k nim je dnes již neoddělitelnou samozřejmostí. V následující kapitole proběhne představení cloudových úložišť s jejich parametry, možností jejich dostupnosti pro uživatele, a v neposlední řadě přehled aktuálních poskytovatelů, včetně uvedení jejich nabízených produktů. Vzhledem k poměrně vysokému počtu pojmů a parametrů, následující kapitola vychází ze zdrojů [30] a [31].

3.1 Parametry

Kategorií parametrů cloudových úložišť existuje celá řada v závislosti na úhlu pohledu, který si zákazník zvolí. Pro účel této práce budou uvedeny parametry z pohledu uživatele daných služeb.

Zpoplatnění

Na trhu existuje obrovské množství produktů cloudových úložišť s různými podmínkami. Mezi nejpodstatnější z nich patří poplatek za užívání. Široká laická veřejnost nejčastěji využívá produktů nejrozšířenějších poskytovatelů, které jsou s jistými omezeními poskytovány zdarma. Často postačí pouhá registrace k získání dostatečného prostoru pro uložení uživatelských dat. Jinde je nutno pozvat k využívání dané služby další uživatele, aby došlo k navýšení prostoru. Další možností jsou promo odkazy, nabízené jako dárky při různých nákupech či jiných internetových činnostech.

Vedle produktů, které jsou k dispozici zdarma, existují i zpoplatněné verze. Takové alternativy jsou hojně využívané převážně ve firemním sektoru, avšak využívány jsou i koncovými uživateli. Poplatek je obvykle účtován za jednotku objemu dat, vzhledem k určitému časovému údobí. Velké společnosti nabízejí i cloudová řešení pro instituce, jako jsou například vzdělávací zařízení, kde se cena domlouvá alternativně na míru.

Objem dat

Volně dostupné cloudové produkty nabízené široké veřejnosti obvykle disponují úložným prostorem o velikosti řádu jednotek GB, s možností navýšení viz. předchozí odstavce. Můžeme se setkat s úložišti, která však dosahují kapacity až desítek či stovek GB, a přesto jsou poskytována zdarma. Takového produkty mají obvykle fixní a předem danou kapacitu úložiště s možností navýšení a řadu dalších omezení.

Zákazníci z řad firemního sektoru obvykle realizují řešení připravená na míru jejich požadavkům, kde je objem dat jednou z položek smlouvy nebo nějakého ekvivalentního dokumentu. Objem dat je v tomto případě omezen pouze možnostmi poskytovatele a požadavky zákazníka.

Rychlost přístupu

Uživatelé, kteří úložiště využívají pouze k uchování základních souborů, jako jsou prezentace, tabulky či textové dokumenty, obvykle nepocítí prodlevu při synchronizaci do cloudu. Takové soubory nezabírají mnoho místa, a tak jejich přenos trvá velmi krátkou dobu, bez ohledu na rychlost přenosu, která je ze strany poskytovatele cloudu podporována. Omezení mohou nastat při synchronizaci většího objemu dat. Příkladem může být větší množství fotografií ve vysoké kvalitě, videosoubory, nebo například velké databázové soubory.

Běžnému uživateli postačuje základní konfigurovaná rychlost přenosu, avšak v praxi se stále více potkáváme s produkty, kde může být rychlost synchronizace kritickým bodem a malé vychýlení může znamenat finanční ztrátu, v krajním případě i ohrožení lidského života. Z tohoto důvodu je před pořízením řešení cloudového úložiště nutno rozvážit potřebnou rychlost přístupu, vzhledem k charakteru nasazení produktu.

Možnosti obnovení souborů (verzování)

V praxi mohou nastat situace, kdy dojde k přepsání korektní verze souboru verzí, která je chybně považována za aktuální („nejnovější“), a je nutno investovat čas a finanční prostředky do znovuvytvoření daného produktu. Dnešní poskytovatelé vzdálených úložišť ve svých produktech nabízí tzv. verzování dat (souborů), které umožňuje kdykoliv přejít na starší verzi stejného souboru bez nutnosti použití externího verzovacího nástroje. Možnosti a podmínky verzování mohou být jedním z parametrů daného produktu.

Sdílení souborů

Další z možných funkcionalit je možnost sdílení dat, uložených v cloudu i mimo něj. Nejpohodlnější a velice rozšířenou variantou je použití odkazu na soubor nebo adresář. Uživatel uloží data na cloud, a poté si nechá vygenerovat odkaz, který předá kompetentním osobám. Příjemce odkazu poté může pohodlně prostřednictvím prohlížeče, nebo po stažení do počítače, data prohlížet, a v případě, že autor přidělí práva i pro editaci, tak navíc upravovat.

Další variantou je pouhé přidělení právům k datům na základě určitého identifikačního údaje (nejčastěji email), přičemž daní uživatelé po přihlášení do služby mohou provádět stejné úkony, jako v předchozím případě. V takovýchto případech je velmi nutná opatrnost a prevence proti zneužití dat a případných osobních údajů v nich.

Maximální velikost souboru

Před pořízením vlastního cloudového řešení je nutné pečlivě zvážit možnosti a požadavky na samotné úložiště vzhledem k charakteru dat, která budou ukládána. Jak již bylo výše zmíněno, na cloudu se velmi často nacházejí pouze základní dokumenty, avšak to není podmínkou. Zákazníci taktéž ukládají objemná data, jako jsou obrazový materiál, videa či velice objemné databáze různých druhů dat.

Aktuální nabídky cloudových řešení často omezují maximální velikost souboru v závislosti na variantě produktu a konkrétním poskytovateli. Nejčastěji bývá velikost omezena variantou produktu. Placené produkty mívají větší maximální velikost oproti variantám, které jsou zdarma, avšak podmínkou to nutně být nemusí. Dále se můžeme setkat s různou velikostí při nahrávání pomocí odlišných nástrojů, jako jsou internetový prohlížeč, či instalovaný klient daného úložiště.

Rozdílové (parciální) updaty

Méně populární, avšak velmi efektivní možností synchronizace dat ve veřejném cloudu jsou tzv. rozdílové updaty. V takovém případě se synchronizují pouze rozdíly v obsahu souborů, nikoliv samotné celé soubory. Příkladem může být velmi objemný databázový soubor, ve kterém změníme jediný záznam. Z podstaty synchronizace by bylo nutné, aby byl nahrán, popř. stažen, celý soubor, avšak takové řešení by bylo z hlediska využití prostředků neefektivní.

Rozdílové updaty řeší tento problém tak, že se odesílá nebo přijímá právě jen upravená část souboru (upravený záznam), bez nutnosti přenosu celého objemu dat. Takové řešení šetří jak systémové prostředky, tak i čas, který by byl nutný k přenosu většího množství informací.

Kooperace v reálném čase

Ve skupině uživatelů, kde probíhá spolupráce na určitém společném projektu, je často typická nutnost sdílet mezi sebou data v reálnem čase. Výše zmíněné sdílení jednotlivých souborů nebo adresářů by bylo při spolupráci na rozsáhlých projektech časové náročné a velmi kontraproduktivní, a tak přichází vhod pohlížet na sdílení z jiného úhlu pohledu.

Sdílení obsahu mezi uživateli bylo nahrazeno variantou sdílení celého vyhrazeného cloudového úložiště. V závislosti na zvoleném druhu přístupu k takovému cloudu se jednotliví uživatelé (např. programátorská skupina, která vytváří společně jeden rozsáhlý projekt) připojí prostřednictvím specializovaného nástroje, obvykle klienta, k danému úložišti, a v reálném čase mohou projekt realizovat, a přitom mít soubory uložené centrálně na jednom místě, s možností vzájemného (úmyslného) zásahu do dat ostatních uživatelů. V takovéto situaci se dá s výhodou využít kombinaci s verzovacím řešením pro kontrolu aktuálnosti souborů.

Přístupy k datům (architektury)

Zbývající část této podkapitoly se opírá o již zmíněnou problematiku, zabývající se o modely nasazení.

Variantou možnosti přístupu k datům na cloudu může být veřejně přístupné sdílení dat. V takovém případě není nutná jakákoliv identifikace uživatele či související přístupová práva, a uživatel, který má zájem o data v takovém úložišti, obvykle použije webové rozhraní pro jejich získání, alternativně si může pomocí přístupových údajů serveru data stáhnout prostřednictvím klienta.

Komunitní varianta je již více omezená a je nutná základní identifikace k přístupu ke společnému úložišti. Nejčastěji se jedná o skupinu uživatelů se společným zájmem, a k přístupu k datům postačí identifikační údaje prokazující příslušnost k takové komunitě (např.: registrace na fóru dané skupiny uživatelů). Data jsou zde obvykle sdílena v podstatě veřejně, avšak přístup je omezen na daný kolektiv lidí.

Nejčastějším způsobem řízení přístupu jsou jednoznačné registrační údaje, po jejich ověření je umožněn přístup k právě jednomu (případně více) cloudovému úložišti, které není ve výchozím stavu sdíleno s nikým jiným. Zde uživatel spravuje vzhledem k možnostem poskytovaného úložiště pouze svůj datový prostor, a nikdo jiný do něj nezasahuje, stejně tak, jako on nezasahuje do prostorů ostatních uživatelů.

3.2 Dostupnost pro uživatele

Jednou z podstat cloudu je možnost přístupu k datům kdykoliv a odkudkoliv. Je důležitá podpora různých zařízení, a s tím souvisejících operačních systémů. Níže proběhne rekapitulace takových možností a variant přístupu k datům

Zařízení

Pracovat s cloudem jde nyní prostřednictvím široké škály zařízení. Hlavním ovládacím prostředkem je samozřejmě osobní počítač, kde je k dispozici největší množství služeb. Pro splnění možností mobility je taktéž podporována řada mobilních zařízení, mezi které se řadí převážně tablety a mobilní telefony. V poslední době je také možné využití například chytrých televizorů s připojením k internetu, na kterých je možná instalace klientské aplikace.

Operační systém

S výše zmíněnou širokou škálou podporovaných zařízení úzce souvisí operační systémy, které jsou na nich provozovány. Při využití klientských aplikací je nutná podpora ideálně všech běžných operačních systémů. Mezi nejčastější z nich patří Microsoft Windows, MacOS či různé linuxové distribuce. Mezi nejčastější mobilní zástupce řadíme Android, Windows Phone, iOS a BlackBerry.

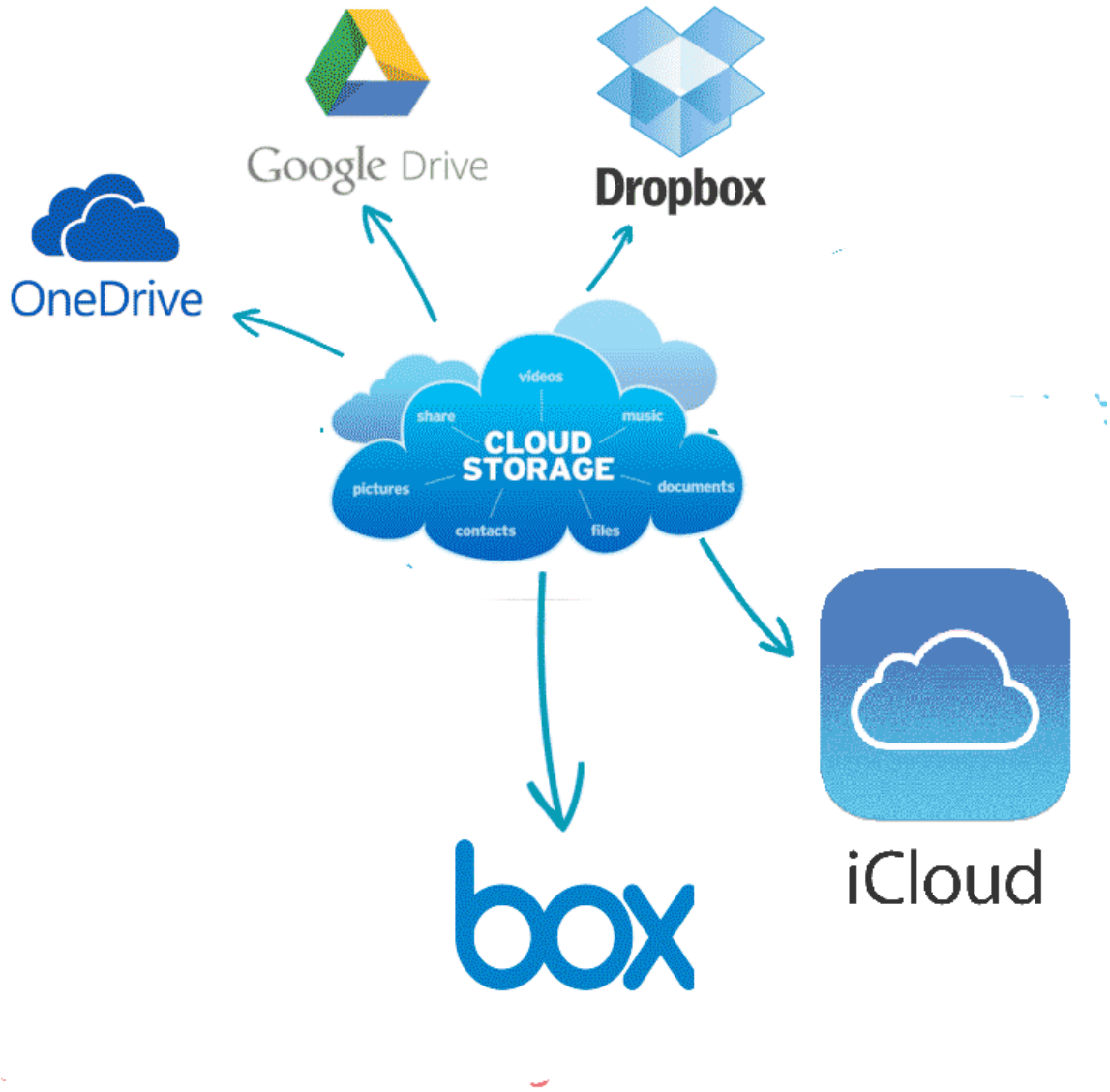
Metoda přístupu

Velmi častou metodou je využití klientské aplikace pro správu dat v úložišti, a to jak při použití počítače, tak i mobilních zařízení. Dále je obvykle možný přístup pomocí běžného prohlížeče po připojení na webové rozhraní daného cloudu.

Obrázek 1 - Ilustrace variací přístupu [59]

3.3 Poskytovatelé

Poskytovateli cloudových úložišť jsou nejčastěji velké firmy působící v oblasti poskytování služeb souvisejících s internetovými službami, které často disponují svým datacentrem. Mezi nejvýznamnější z nich patří technologické firmy jako například: Microsoft (OneDrive), Google (Google Drive), Apple (iCloud), či například Dropbox (Dropbox) a velké množství dalších. Dále se můžeme setkat s řadou menších poskytovatelů se zajímavou nabídkou [7].



Obrázek 2 - Ilustrace poskytovatelů [8]

4 AKTUÁLNÍ PRODUKTY (CLOUDOVÁ ÚLOŽIŠTĚ)

V následující kapitole proběhne srovnání několika nynějších cloudových úložišť. Zkoumána bude cena, podmínky registrace s požadavky a zabezpečení poskytované ve výchozím stavu.

4.1 Google Drive

Google Drive je produkt celosvětové společnosti Google a řadí se mezi nejpopulárnější zástupce z řad cloudových produktů po téměř celém světě. Zahrnuje taktéž kancelářské nástroje Google Docs, které je možno provozovat přímo v prohlížeči [38].

Cena

Předplatné je možno financovat buď měsíčně nebo ročně [52].

- 15 GB / zdarma
- 100 GB / 59,99 Kč (měsíc), 599,99 Kč (rok)
- 1 TB / 299,99 Kč (měsíc), 2999,99 Kč (rok)
- 2 TB / 599,99 Kč (měsíc)
- 10 TB / 2999,99 Kč (měsíc)
- 20 TB / 5999,99 Kč (měsíc)

Podmínky registrace

Základem k užívání je platný účet u společnosti Google. Dále je nutno splňovat některé další podmínky. Jedná se o druh prohlížeče, podporované operační systémy, a to jak mobilní, tak i desktopové. Tyto podmínky platí, až na výjimky, u všech cloudových produktů. Níže uvedené prohlížeče jsou podporovány po dvě verze zpětně, ostatní bez garance funkčnosti všech součástí. Nutné povolení cookies a JavaScriptu [44].

- Google Chrome (novější než verze 23)
- Mozilla Firefox (novější než verze 23)
- Internet Explorer (novější než verze 9), Microsoft Edge (oba pouze pro Windows)
- Safari (pouze pro Mac, novější než verze 6)

Mezi podporované desktopové operační systémy patři ty nejběžnější s výjimkou Linuxu.

- Windows (Windows Vista a novější)
- Max (10.7 Lion a novější)
- Linux (pouze prostřednictvím prohlížeče)

Mezi podporované mobilní operační systémy patři Android a iOS

- Android (4.4 a novější)
  iOS (9.0 a novější)

Poskytované zabezpečení dat

Google Drive nabízí velmi dobrou úroveň zabezpečení. Servery podporují šifrování AES-256 pro uložená data. Využívá se dvoufázové ověřování a připojení je chráněno pomocí SSL/TLS tunelů. Produkt je certifikován podle ISO 27001. Dalšími prvky jsou bezpečnostní upozornění a nástroje pro správu soukromí a sdílení [26].

4.2 Dropbox

Dropbox je cloudové úložiště spravované společností Dropbox, Inc. Taktéž patří mezi největší populární cloudová řešení [22].

Cena

Předplatné začíná na úrovni Dropbox Basic, které je zdarma a poskytuje 2 GB volného prostoru. Dále je možnost zakoupení Dropbox Plus, které nabízí 1 TB volného místa a některé další funkce. Měsíc využívání stojí při platě měsíčně 9,99 EUR za měsíc, při platbě ročně 99,00 EUR. Dále je možnost využití funkce pro rozšířenou historii verzí, která umožňuje verzovat soubory a smazaná data po dobu jednoho roku bez zabírání prostoru úložiště. Poplatek za tuto funkcionalitu činí 39,99 EUR na dobu jednoho roku.

Pokročilejší variantou úložiště je Dropbox Business, jejíž cena záleží na velikosti skupiny, pro kterou je cloud určen a finančních možnostech dané instituce. Dropbox poskytuje slevy pro neziskové organizace a vzdělávací zařízení [29].

Podmínky registrace

Prvotním požadavkem je registrovaný účet na Dropboxu, alternativně je možné přihlášení prostřednictvím účtu Google [46].

Dropbox také garantuje funkčnost u posledních dvou verzí následujících prohlížečů.

- Google Chrome
- Mozilla Firefox
- Microsoft Edge, Internet Explorer
- Safari

Co se týče desktopových operačních systémů, Dropbox přidává podporu některých linuxových distribucí.

- Windows (Vista, 7, 8, 8.1, 9, 10)
- Mac (OS X 10.6.8 Snow Leopard až macOS 10.12 Sierra)
- Linux (Ubuntu 10.04 a vyšší, Fedora 19 a vyšší)

Mobilní operační systémy jsou zde rozšířeny o podporu systému Microsoft Windows.

- iOS (9 a novější)
- Android (4.1 a novější)
- Windows Phone (8.0 a novější), Windows tablet (8.1 nebo RT)
- Windows tablet

Poskytované zabezpečení dat

Podobně jako předchozí produkt, se i Dropbox může pochlubit šifrováním AES-256 na svých serverech. Přenos taktéž probíhá pomocí tunelů SSL/TLS, ověření je dvoufázové a jsou možná bezpečnostní upozornění. Mimo certifikace ISO 27001 zde můžeme narazit na certifikaci ISO 27018. Navíc existuje možnost monitorování uživatelů a neomezeného obnovení dat [26].

4.3 Amazon Drive (Cloud Drive)

V České republice se jedná o méně populární, avšak globálně se řadí do kategorie populárních produktů vzdálených úložišť.

Cena

Amazon již nenabízí úložiště zdarma (dříve se jednalo o 5 GB prostoru), takže v případě volby tohoto poskytovatele bude nutné zvolit jednu z placených variant.

První z nich je Prime Photos, které poskytuje neomezený prostor pro fotografie a 5 GB pro ostatní uživatelská data. Pro získání přístupu k úložišti je nutné vlastnictví účtu se zaplaceným předplatným Amazon Prime, které stojí měsíčně 10,99 USD a ročně 99 USD [3].

Další možností je neomezené úložiště, jehož pořízení je zpoplatněné částkou 59,99 USD za rok užívání, s možností tří měsíců, které slouží k vyzkoušení zdarma [5].

Podmínky registrace

Informace o podmínkách registrace a využívání tohoto produktu byly čerpány ze stránek společnosti Amazon. Konkrétně pak zdroje [1], [2] a [54].

V případě neplacené alternativy produktu je nutný účet Amazon Prime, který však již zpoplatněn je. U běžně zpoplatněné neomezené alternativy již postačí klasický Amazon účet.

Webové nahrávání vyžaduje pro zachování funkčnosti z důvodu využití HTML 5, určité verze prohlížečů.

- Google Chrome (podpora nahrávání celých složek od verze 21 a novější)
- Mozilla Firefox (4 a novější)
- Microsoft Edge (podpora nahrávání celých složek), Internet Explorer (10 a novější)
- Safari (6 a novější pro desktop, 6.1 a novější pro mobilní zařízení)
- Opera (desktop neuveden, 12 a novější pro mobilní zařízení)

Aplikace pro desktop bohužel není podporována na Linuxu, na dalších desktopových systémech však ano.

- Windows (7 a novější)
- Mac (OS X 10.10 a novější)

V oblasti mobilních zařízení přibyla podpora tabletů společnosti Kindle.

- Android (4.2 a novější)
- iOS (8 a novější)

Fire Tablets (s výjimkou Kindle Fire 1st Generation)

Poskytované zabezpečení dat

I přesto, že Amazon provozuje úložiště na serverech, které sami vlastní, nejsou uložená data na samotných serverech šifrována. Přenos souborů je však zabezpečen protokolem SSL. Problém se ale nachází v podmínkách soukromí, kde Amazon naznačuje, že služba kdykoliv může číst veškerá uživatelská data, a mimo jiné je může poskytnout pro potřeby technické podpory. Ve skutečnosti podmínky přenáší bezpečnostní zodpovědnost na uživatele, kde je uživatel zodpovědný za odpovídající ochranu a bezpečnost uložených dat, což je v rozporu službami zabezpečených cloudových úložišť. Dále však Amazon poskytuje na svém úložišti dvoufázové ověřování, které se používá ve variantách, kde se určitý potvrzovací kód předá prostřednictvím SMS, emailu nebo třeba telefonního hovoru [40].

4.4 Microsoft OneDrive

Microsoft OneDrive, dříve SkyDrive, je úložiště spravované společností Microsoft a jeho podpora je směřována převážně do operačních systémů od stejnojmenné společnosti [32].

Cena

Úložiště je součástí několika nabídek, které obsahují funkce společnosti Microsoft, avšak zde budou uvedeny tarify pouze za využívání samostatného úložiště.

OneDrive je pro jednotlivé uživatele nabízen ve variantě OneDrive Basic, které je poskytováno ve velikosti 5 GB zdarma a variantě OneDrive, která je zpoplatněna částkou 49,99 Kč za měsíc a poskytující 50 GB úložného prostoru.

Pro firemní zákazníky existuje varianta OneDrive pro firmy, která stojí firmu 50,40 EUR za rok využívání a poskytuje 1 TB pro každého uživatele. Druhou možností je OneDrive Business Advanced, která stojí dvojnásobek a nabízí taktéž 1 TB úložného prostoru, který se však při více než pěti uživatelích mění na neomezený [49].

Podmínky registrace

Základní podmínkou využívání je účet u společnosti Microsoft. OneDrive přichází s podporou běžně používaných prohlížečů a mobilních i desktopových operačních systémů.

Jsou doporučeny pouze jednotlivé prohlížeče, bez specifikace verzí [39].

- Google Chrome
- Mozilla Firefox
- Internet Explorer, Microsoft Edge
- Safari

U operačních systémů přibývá podpora pro některé serverové operační systémy. Převažují samozřejmě produkty společnosti Microsoft.

- Windows (Vista 7, 8, 8.1, 10)
- Windows Server (2012, 2008 R2, 2008 SP2)
- Mac (OS X 10.9 a vyšší)

U mobilních operačních systémů je samozřejmostí podpora pro Windows Phone.

- Android (2.3 a novější), Android (4.0 a novější) pro podporu některých funkcionalit navíc
- iOS (9.0 a novější)
- Windows Phone (7.5 a novější)

Poskytované zabezpečení dat

Vzhledem k vyššímu počtu rozdílných informací bylo čerpáno ze zdrojů [27], [41] a [61].

Přenášená data jsou zabezpečena pomocí protokolu SSL 128-bit, ale pouze v případě varianty OneDrive Business, zabezpečení v podobě šifrování na úrovni AES-256 zůstává i při jejich uložení na serveru. OneDrive Business také nabízí možnost šifrovat zvlášť po souborech, což zvyšuje bezpečnost. Samozřejmostí je dvoufázové ověření bez omezení typu produktu. I OneDrive skrývá úskalí spojená se soukromím, protože si společnost Microsoft vyhrazuje právo k procházení uživatelských dat z důvodu hledání nevhodného obsahu. Tato činnost může vést až ke smazání dat, která jsou jako nevhodný obsah označena.

4.5 iCloud Drive

iCloud je cloud, který provozuje společnost Apple, a taktéž se jedná o velkého zástupce z řad poskytování cloudových produktů. Vzhledem k podpoře je populární zejména mezi uživateli produktů výrobce Apple [14].

Cena

iCloud poskytuje 5 GB volného prostoru zdarma. Za měsíční poplatek je možno prostor navýšit [13].

- 50 GB / 0,99 EUR
- 200 GB / 2,99 EUR
- 1 TB / 9,99 EUR
- 2 TB / 19,99 EUR

Podmínky registrace

Využívání služeb iCloud vyžaduje aktivní Apple ID. Zde je zajímavostí podpora zařízení Apple TV.

Podpora prohlížečů a operačních systémů se u jednotlivých součástí liší. Detailní přehled lze nalézt ve zdroji [45]. Následuje stručný souhrn minimálních požadavků po platformách.

Mezi podporované desktopové operační systémy a další nutné součásti patři níže uvedené produkty.

- zařízení typu iPhone, iPod a iPad
    - iOS (verze 10.3 a novější)
    - iWork pro platformu iOS
- Mac
    - macOS Sierra
    - iTunes 12.5
    - prohlížeče
        - Safari (9.1 a novější)
        - Mozilla Firefox (verze 45 a novější)
        - Google Chrome (verze 54 a novější)
    - iWork pro platformu Mac
- Běžné počítače
    - Windows 10
    - iCloud (verze 6) pro platformu Windows
    - iTunes 12.5
    - Outlook (2007 do verze 2016)
    - prohlížeče
        - Google Chrome (verze 54 a novější)
        - Mozilla Firefox (verze 45 a novější)
        - Internet Explorer (verze 11 a novější)
- Apple TV (verze 7.2.1 a novější)

Poskytované zabezpečení dat

Společnost uvádí, že přenos uživatelských dat je zabezpečen prostřednictvím protokolu SSL. Taktéž data uložená na serveru jsou chráněna, a to 128bitovým šifrováním AES. Dalším prvkem zabezpečení je iCloud klíčenka, která je využita pro uložení a přenos hesel a údajů k platebním kartám s použitím 256bitového AES šifrování. Samozřejmostí je dvoufázové, resp. dvoufaktorové ověřování a tokeny, které zabezpečují ověření [61].

4.6 MEGA

MEGA je vzdálené cloudové úložiště, vyvíjené společností Mega Ltd [34].

Cena

MEGA nabízí ve srovnání s ostatními dostatek volného prostoru již ve verzi, která je zdarma, a to 50 GB.

Mezi placené verze patří Lite, která za 4,99 EUR za měsíc, nabízí 200 GB. PRO I poskytuje za 9,99 EUR měsíčně, prostor o velikosti 500 GB. PRO II nabídne za 19,99 EUR celé 2 TB, a nakonec PRO III, které za 29,99 EUR nabízí úložiště o objemu 4 TB. Pokud si uživatel zakoupí roční předplatné verze PRO, získá tím 2 měsíce zdarma. Každá z variant má různou kvótu přenosu, což znamená měsíční objem dat přenesených mezi servery MEGA a uživatelem [36].

Podmínky registrace

Jedinou podmínkou pro využívání produktu MEGA je registrace a s ní související účet na stránkách úložiště [28].

Využívat je možno nejčastější internetové prohlížeče s podporou HTML 5. V případě zájmu zvýšené bezpečnosti, rychlosti a vylepšení práce s objemnými soubory je nutno nainstalovat doplněk pro prohlížeče Google Chrome nebo Mozilla Firefox. Pro práci s objemnými soubory je doporučeno nainstalovat přímo klientskou aplikaci MEGAsync, protože prohlížeče trpí paměťovým omezením, a s tím souvisí případné problémy při end-to-end šifrování. Níže jsou uvedeny nejvíce kompatibilní internetové prohlížeče. Není vyloučena funkčnost i v jiných prohlížečích, avšak bez garance plné funkcionality [58].

- Google Chrome
- Opera
- Mozilla Firefox (nutno nainstalovat doplněk do prohlížeče pro plnou funkčnost)

Klientská aplikace MEGAsync je taktéž podporována pro běžně používané desktopové platformy [37].

- Microsoft Windows
- Linux
- Mac

Mobilní aplikace přidává k běžně využívaným platformám také podporu BlackBerry [35].

- Android
- iOS
- Windows Phone
- BlackBerry

Poskytované zabezpečení dat

MEGA úložiště je známo svým přístupem k zabezpečení a soukromí dat. Poskytuje šifrování, které je řízeno uživatelem a 2048bitové RSA end-to-end šifrování, jak pro soukromý, tak i veřejný klíč. Data jsou uložena jak na serveru, tak i cestou k němu. MEGA neudržuje dešifrovací klíče, takže tato zodpovědnost připadá na uživatele úložiště. Stejně tak neukládá uživatelská jména a hesla, takže v případě žádosti o obnovení náhodně generovaného kódu, který byl získán při registraci, nastane příležitost pro uložení hlavního klíče, tak jako jeho opětovné stažení po přihlášení. I zde připadá zodpovědnost na stranu uživatele, protože v případě ztráty neexistuje jiná možnost, než kompletní vymazání účtu a založení nového. Soubory je možné sdílet i s neregistrovanými uživateli, a to s využitím unikátních klíčů. V případě kolaborace více uživatelů je však nutná registrace [18].

4.7 Wedos Disk

Wedos Disk je jediný český zástupce tomto srovnání a je provozován společností WEDOS Internet, a.s. Wedos se řadí v rámci nabízených internetových služeb, poskytovaných na území České republiky, mezi přední zástupce, a taktéž poskytuje cloudové úložiště [57].

Cena

Navzdory menšímu rozsahu české společnosti Wedos (oproti celosvětovým společnostem) je Wedos Disk zajímavým cloudovým řešením. Základní varianta je dostupná zdarma za podmínky zakoupení služeb webhostingu nebo VPS, a to s kapacitou až 10 GB. 30 GB je k dostání za 2,18 EUR měsíčně, 100 GB lze získat za 4,36 EUR měsíčně a prostor s minimální kapacitou 1 TB stojí 13,19 EUR za měsíc využívání [57].

Podmínky registrace

Jak již bylo dříve uvedeno, podmínkou bezplatného využívání tohoto úložiště je aktivní webhosting. Možné je taktéž zpoplatněné využívání samostatného úložného prostoru.

Jelikož společnost nenabízí vlastního aplikačního klienta, je nutné využít běžně používané protokoly, a s nimi související služby, pro přístup k souborům na úložišti. Další možností jsou doplňky do prohlížečů nebo jiné produkty třetích stran, které jsou určeny pro vzdálený přístup k datům. Následuje výčet podporovaných služeb a protokolů [51].

- FTP
- rsync
- SMB (CIFS)

Kompletní informace o možnostech a parametrech přístupu lze nalézt ve znalostní bázi na stránkách poskytovatele.

Poskytované zabezpečení dat

Vzhledem k faktu, že se jedná o produkt české společnosti, nebyl dostupný takový objem informací, jako u jiných, celosvětových produktů. Čerpáno bylo tudíž pouze přímo ze stránek poskytovatele a byla zjištěna níže uvedená fakta.

Data mohou být přenášena šifrovanou komunikací, ale přímo na serveru šifrována nejsou. K tomu se s výhodou používá nástrojů třetích stran, které budou představený později v této práci. Samozřejmostí je firewall, který je použit na serverech úložiště [51].

4.8 Shrnutí

Základní podmínkou využívání služeb úložiště je v drtivé většině případů pouze registrace na stránkách poskytovatele. Jednotlivé produkty se pak obvykle liší určitými podmínkami, které je pro práci s daným produktem nutno dodržet.

Vzhledem k již velmi vysoké úrovni poskytované ochrany dat, často není třeba dokupovat vyšší možnosti zabezpečení. Zároveň se často jedná o méně přístupnou konkrétní možnost a běžně není poskytována. V případě potřeby lze s výhodou využít externí nástroje třetích stran, které budou představeny později.

Poskytovatelé nabízejí ochranu dat na velmi dobré úrovni. Existuje však riziko, které nelze plně eliminovat a nazývá se lidský faktor. Uživatel totiž může velmi snadno udělat chybu v nastavení soukromí a sdílení na úložišti, či předat přístupové údaje neoprávněné osobě, a tak snadno dochází ke krádeži dat. Uživatelé často tako využívají neoficiální nástroje pro práci s daty, které mohou taktéž být bezpečnostními hrozbami.

V následující tabulce jsou shrnuty některé parametry produktů a jejich hodnoty, kterých nabývají v případě získáni 15GB úložného prostoru pro neomezený druh dat a běžného koncového uživatele.

Tabulka 1 - Srovnání produktů cloudových úložišť

Produkt	Cena	Šifrování dat na serveru	Podpora mobilních zařízení	Poznámka (specifikum)
Google Drive	zdarma (až do 15 GB)	AES-256	Android, iOS	15 GB zdarma
Dropbox	9,99 EUR za měsíc	AES-256	Android, iOS, Windows Phone (navíc tablety Windows)	možnost přizvat další účastníky za další prostor zdarma, podpora Linuxu
Amazon Drive	první 3 měsíce zdarma, poté 59,99 USD za rok	není poskytováno	Android, iOS, FireTablets	podpora tabletů FireTablets
Microsoft OneDrive	49,99 Kč za měsíc	pouze u OneDrive Business (AES-256)	Android, iOS, Windows Phone	právo prohledávat data z důvodu hledání nevhodného obsahu
iCloud Drive	0,99 EUR za měsíc	AES-128	iOS	podpora AppleTV
MEGA	zdarma (až do 50 GB)	ano (vysoká úroveň, neuvedena konkrétně)	Android, iOS, Windows Phone, BlackBerry	velmi vysoká úroveň zabezpečení, velikost úložiště zdarma
Wedos Disk	2,18 EUR za měsíc	není poskytováno	není podporováno	český produkt

Při zpětném pohledu na informace uvedené v této kapitole vyplývá tvrzení, že čisté zabezpečení dat v cloudu v podstatě nejsme schopni kontrolovat a samotná data zabezpečit. Z tohoto důvodu se nabízí možnost využití nástrojů třetích stran, které budou představeny dále v této práci.

5 ŠIFROVÁNÍ

Šifrování dat je možno chápat jako převod dat, která nejsou nijak zabezpečena, do podoby, která zajišťuje jejich nečitelnost a ochranu proti neoprávněnému přístupu. Obecně jsou data přístupná pouze pro subjekty, které mají k dispozici šifrovací klíč. Základní jednotkou délky šifrovacího klíče je bit. Délka klíče je závislá na použitém algoritmu a cíli určení, resp. důležitosti dat, která mají být šifrována. Takovýto převod dat se nazývá kryptografie a dělí se na velké množství různých odvětví. V následující kapitole proběhne představení informací, které se šifrováním přímo souvisí. Následující kapitola čerpá převážně ze zdrojů [47] a [48].

5.1 Typy šifrování

V základním pojetí šifrování se setkáváme s dvěma typy, kterými jsou symetrické a asymetrické. Jedná se o šifry s rozdílnými parametry a níže proběhne jejich představení [48].

Symetrické šifrování

Charakteristickou vlastností je totožný šifrovací i dešifrovací klíč. V případě využití dvou různých klíčů je nutná přítomnost možnosti výpočtu druhého klíče z prvního a naopak. V tomto případě nejčastěji jedna strana vytvoří šifrovací klíč, který je poté pomocí asymetrické šifry bezpečně doručen straně druhé. Z toho plyne obvyklá souběžnosti obou šifrovacích typů.

Negativním faktem je nutnost množství šifrovacích klíčů, v závislosti na počtu účastníků komunikace. V případě, že uživatel chce, aby odeslaná data přečetl pouze jeden konkrétní příjemce, a zároveň chce komunikovat se všemi účastníky, potřebuje celkem N*(N-1) / 2 šifrovacích klíčů, kde N představuje počet účastníků komunikace. V případě asymetrické varianty je tento počet snížen na 2*N.

Poslední podstatnou charakteristikou je nemožnost rozeznání strany, která data vytvořila, protože obě komunikující strany mají stejný šifrovací klíč.

Oproti asymetrickému šifrování je tento způsob rychlejší.

Symetrické šifry existují v těchto variantách: DES, 3DES1 AES, IDEA, RC4 a další [48].

Asymetrické šifrování

V porovnání se symetrickou šifrou tato šifra využívá klíče dva. Jmenují se public (veřejný) a private (privátní).

Privátní klíč je identifikací a charakteristikou vlastníka a jedná se o citlivý údaj. Veřejný klíč naopak druhý účastník komunikace znát musí. Tyto klíče jsou na sebe navázány v páru.

Pár klíčů se generuje v jednom okamžiku souběžně, jednotlivé klíče jsou na sobě závislé pomocí matematických postupů. Existuje způsob, kterým se z veřejného klíče dá složitými matematickými operacemi vypočítat klíč privátní, ale při délce šifrovacích klíčů je to v dnešní době téměř nemožné. Šifrování s větší délkou klíče se používá v místech, jako jsou banky a armáda, kde se pracuje se skutečné citlivými daty.

Komunikace probíhá tak, že si komunikující strany vytvoří pár šifrovacích klíčů, přičemž vlastní veřejný klíč doručí druhé straně. Přenášená data jsou pak zašifrována privátním šifrovacích klíčem, odeslána směrem k příjemci, který je veřejným klíčem dešifruje.

Nejčastějšími zástupci asymetrických šifer jsou: RSA, DSA, DH, ECDSA a další [48].

6 ŠIFROVÁNÍ DAT V CLOUDU

Existují postupy, zvyšující úroveň zabezpečení dat, která jsou umístěna v úložišti. Řešení mohou být rozdělena například na interní a externí. Do interních řešení mohou být zařazeny veškeré formy zabezpečení a šifrování, které poskytovatel služeb implementuje již do samotného úložiště. Druhou možností jsou externí nástroje třetích stran, které mohou zvýšit úroveň zabezpečení dat již na straně uživatele, ještě před odesláním na úložiště. V této kapitole proběhne představení a přehled několika takovýchto řešení.

6.1 Nástroje třetích stran

Řešení pomocí nástrojů třetích stran v podstatě vždy vyžadují instalaci programu, který zajišťuje šifrování, a poté správu šifrovaných dat. Samotný proces může mít poměrně velké požadavky na systémové prostředky, záleží však na konkrétním případě, typu a velikosti dat. Produktů pro obecné šifrování dat existuje celá škála, v této práci však bude analýza zaměřena na programy, které pracuji se zabezpečením a šifrováním přímo cloudových dat.

6.2 Boxcryptor

Charakteristika

Boxcryptor je software, který se využívá k šifrování dat na cloudovém úložišti. Byl vyvinut německou společností Secomba GmbH a řadí se mezi nejpopulárnější produkty své kategorie. Vždy se používá v kombinaci s určitým řešením cloudového úložiště a v současné době podporuje velké množství běžných i méně populárních cloudů. Seznam je k nalezení na stránkách produktu: [4]. Boxcryptor je navržen podle zero knowledge paradigmatu, což znamená, že k datům v daném případě má přístup pouze jejich vlastník, a nikdo jiný k nim nesmí přistupovat. Samozřejmostí je podpora široké škály jak mobilních, tak i desktopových platforem. Boxcryptor kombinuje možnosti asymetrických i symetrických šifer. Každý soubor má svůj vlastní, náhodně generovaný klíč, který vznikne při vytvoření souboru a používá se k šifrování a dešifrování samotných dat souboru. Použitými základními algoritmy jsou 256bitová varianta AES v kombinaci s CBC a PKCS7, dále pak 4096bitová varianta RSA v kombinaci s OAEP. Detailní popis technických údajů je k dispozici na stránkách produktu: [50]. Kapitola čerpá většinu informací z jednotlivých stránek webu poskytovatele, konkrétně pak: [10], [11], [12] a [24].

Požadavky

Boxcryptor podporuje velké množství jak mobilních, tak desktopových platforem.

- Windows (verze 7, 8, 10)
- macOS (verze 10.9 a vyšší)
- Android (verze 4.0.3 a vyšší)
- iOS (verze 8.2 a vyšší)
- Windows Phone (verze 8 a vyšší)
- Blackberry OS (10. 2 a vyšší)

Dále je k dispozici portable varianta pro 64bitové varianty Linuxu a macOS, dále pak 32bitové Windows, a nakonec je dostupný doplněk do prohlížeče Google Chrome [20].

Samozřejmou podmínkou, která je nutná pro využívání je internetové připojení. Obecné požadavky na hardware výrobce neuvádí. Vzhledem k výpočetní náročnosti při šifrování však platí, že čím výkonnější zařízení, tím rychleji celkový proces proběhne.

Zpoplatnění (licence, varianty)

Boxcryptor je nabízen ve verzích pro jednotlivce nebo skupiny. První z nich je s určitými omezeními v základní verzi dostupná zdarma pro nekomerční využití. Dále jsou možnosti zakoupení licence bez omezení pro jednotlivé koncové uživatele. Cena se pohybuje okolo 36 EUR za rok pro osobní využití, dvojnásobek pro komerční, a nakonec varianta pro hromadné firemní použití, kde se platí 6,40 EUR za měsíc a uživatele [11].

Druhou variantou je licence pro skupiny, kde jsou rozšířené možnosti spolupráce mezi uživateli v rámci skupiny. Cena se zde odvíjí v závislosti na počtu uživatelů a letech, na které je licence zakoupena [12].

6.3 Cryptomator

Charakteristika

Obecné informace pro sestavení charakteristiky jsou čerpány ze zdrojů [9] a [42].

Cryptomator je další z řady externích nástrojů, které se dají použít pro zašifrování osobních dat na cloudovém úložišti. Je to produkt z rukou německých vývojářů a jedná se o velmi solidní produkt svého druhu, který nabízí mnohá zabezpečení. První funkcionalitou je virtuální souborový systém, který zajišťuje, že nikde na disku nejsou žádné nezašifrované kopie uživatelských dat. Služba SHA1PRNG se stará o náhodné generování šifrovacích klíčů. Další vrstvou ochrany je hlavní klíč, který je sám o sobě zabezpečen uživatelským heslem.

Jednotlivé šifrované soubory mají svůj vlastní šifrovací klíč, který je navíc zabezpečený klíčem hlavním. Zajímavostí je oddělené šifrování názvu souboru, hlavičky souboru, a nakonec samotného datového obsahu. Použitými algoritmy jsou AES-CTR v kombinaci s AES-SIV. Klíče jsou soustředěny v tzv. trezoru a veškerá data v něm jsou zabezpečena. Přístup k němu je možný pomocí hesla uživatele. Cryptomator není závislý na samotných cloudových úložištích. Stačí pouze vložit danou šifrovanou datovou jednotku (trezor) do složky úložiště a zbytek procesu probíhá jako při běžné synchronizaci obyčejných souborů. Jednotlivé trezory jsou šifrovány již zmíněným 256bitovým algoritmem.

Požadavky

Podporované operační systémy konečně zahrnují také systém Linux, který je často opomíjen.

- Windows (Windows Vista SP2 a vyšší)
- Mac (OS X 10.8.3)
- Linux (různé u jednotlivých distribucí)
- ostatní platformy založené podporující Javu

Mobilní aplikace bohužel pokulhávají a výsledkem je pouze varianta pro Android, která je ve verzi beta, a navíc s velice omezenými možnostmi.

Hardwarové požadavky taktéž nejsou uvedeny, ale zpravidla platí totéž, co je uvedeno u předchozího produktu.

Výše uvedené požadavky byly sepsány na základě informací, které byly nalezeny ve zdrojích [9] a [21].

Zpoplatnění (licence, varianty)

Cryptomator je produkt, který je nabízen zcela zdarma v jedné variantě. Výrobce dává na svých stránkách možnost dobrovolného poplatku za stažení aplikace [17].

6.4 Viivo

Charakteristika

Viivo je další z řady produktů, které slouží pro zabezpečení uživatelských da v cloudu. Řešení od společnosti PKWARE před odesláním na cloud data nejdříve zabezpečí, a až poté je umožní synchronizovat, což zvyšuje ochranu před zneužitím a neoprávněným přečtením dat. Servery provozovatele nikdy nemají přístup k nezašifrovaným kopiím uložených dat, stejně tak ke klíčům. Uživatel sám spravuje klíče, kterými jsou data zabezpečena. Viivo využívá několik vrstev šifrování.

Na první úrovni probíhá výměna párů klíčů, které jsou šifrovány 2048bitovou variantou RSA algoritmu. Uživatelský privátní RSA klíč je zabezpečen heslem, které si uživatel zvolí. Heslo je zabezpečeno silnou kombinací PBKDF2, HMAC, a SHA256. Nakonec jsou zašifrovány samotné soubory algoritmem AES o délce klíče 256 bitů. V případě sdílení zabezpečených souborů je každý soubor zvlášť šifrován náhodně vygenerovaným, unikátním relačním šifrovacím klíčem. Tento klíč je použit pouze pro jeden soubor, a nikdy žádný jiný. Software spolupracuje s řadou populárních úložišť, mezi které se řadí hlavně Dropbox, Box, Google Drive, Microsoft OneDrive. Zajímavostí je možnost nasazení v privátních cloudech. Program se taktéž stará o kompresi dat, aby došlo k úspoře místa na úložišti [55].

Požadavky

Viivo na rozdíl od ostatních produktů nedisponuje tak rozsáhlým množstvím podporovaných platforem.

- Mac OS
- Windows
- iOS
- Android

S hardwarovými požadavky je to stejné jako v předchozích případech [55].

Zpoplatnění (licence, varianty)

Varianta pro nekomerční osobní využití je dostupná zdarma. V případě komerční je zdarma 14 dní využívání, poté je nutno upgradovat na vybranou variantu [53].

- Viivo Pro
    - komerční využití
    - rozšířené funkcionality
    - zpoplatněno měsíčně nebo ročně
- Viivo Business
    - funkcionality verze Pro
    - navíc rozšířené možnosti pro správce
    - poplatek předmětem konkrétní nabídky na míru

6.5 Shrnutí nástrojů

Na trhu existuje celá řada nástrojů pro zabezpečení souborů, a to nejen pro cloudové využití. Výhodou využití výše zmíněného druhu nástrojů je možnost přidání několika dalších vrstev zabezpečení, které exponenciálně zvyšují kvalitu zabezpečení souborů, čímž chrání i velmi citlivá data. Za zmínku zde stojí jistě výše představené úložiště MEGA, které již mnoho z těchto principů uplatňuje v samotném synchronizačním klientovi. Produkty jsou často nabízeny v základní verzi zdarma, což pro běžné používání vzhledem k již velmi vysokému zabezpečení bohatě stačí. V případě placených variant je nutné uhrazení poplatku, který se může zdát poměrně vysoký. Podstatnější nevýhodou jsou jistě hardwarové požadavky, což není běžně uváděná informace, ale jak již bylo zmíněno, z logické úvahy nad principem šifrování se jedná o výpočetně náročné procesy a v kombinaci s požadavkem na kvalitnější internetové připojení mohou mít někteří uživatelé prodlevy při vykonávání daných činností. Útěchou může být obecně solidní podpora mnoha platforem běžně užívaných zařízení.

6.6 Zabezpečení na úrovni úložiště (interní nástroje)

Zabezpečení poskytované poskytovatelem cloudu bohužel není pro uživatele transparentní. Zpravidla jsou uvedeny základní informace o vrstvách zabezpečení a použitých algoritmech, ale konkrétní parametry a interní funkcionality jsou z pochopitelných důvodů veřejnosti zatajeny. V předchozích kapitolách byly způsoby a konkrétní řešení takovýchto nástrojů pro zabezpečení popsány na jednotlivých cloudových produktech.

Porovnání

Interní nástroje nabízí v dnešní době velmi slušnou úroveň zabezpečení, které však často komplikují podmínky ujednání při registraci na stránkách poskytovatele, ve kterých se uživatel musí zavázat k souhlasu poskytnutí svých dat provozovateli k různým účelům, což není mnohdy vhodné. Z tohoto důvodu je výhodné použití šifrovacího nástroje pro znemožnění přečtení nepovolaným subjektem. Systémové požadavky zde však nejsou tak vysoké, protože vzhledem k absenci nutnosti nástroje, který zajišťuje šifrování, a tím pádem spotřebovává výkon zařízení, stačí pouze klient, pomocí kterého se synchronizují data na samotné úložiště. V mnoha případech postačí pouze internetový prohlížeč.

6.7 Shrnutí kapitoly

Využívání cloudového úložiště je praktickým a moderním způsobem ukládání uživatelských dat. Hojně se používá téměř ve všech průmyslových i neprůmyslových odvětvích, a samozřejmě také pro osobní použití. S rostoucí rychlostí vývoje technologií se zvyšují i pokusy o krádeže dat a prolomení ochrany, k čemuž je nutno využít známých i méně známých algoritmů a principů, které jsou představeny v teoretické části této práce. Poskytovatelé úložiště již interně chrání data tak, aby k nim neměl žádný neoprávněný subjekt přístup, ale ne vždy úspěšně. Takovým případům se dá bránit pomocí nástrojů a různých druhů řešení, která přidávají další vrstvy zabezpečení, a tím více data chrání. Nakonec je nutné brát v úvahu lidský faktor, který se v mnoha případech nijak ošetřit nedá, a chyba, kterou člověk pří provozu na zařízeních a internetu způsobí, může mít bez ohledu na implementované zabezpečení, fatální dopad.

7 ANALÝZA NÁSTROJŮ PRO ZABEZPEČENÍ DAT

Tato kapitola je praktickou částí zmíněné bakalářské práce.

7.1 Interní nástroje úložišť

Vzhledem k charakteru interních nástrojů, zde není možno měřit zatížení serveru, který provádí šifrování a celkovou ochranu uložených dat (pokud ji server poskytuje). Zabezpečení samozřejmě proběhne podle podmínek, kterými se produkt řídi, ale v tomto případě není způsob, kterým by se analýza využití prostředků dala realizovat.

7.2 Popis praktické části (externí nástroje)

Předmětem následující části je analýza využití systémových prostředků a činnosti procesu zabezpečení a synchronizace dat, která budou šifrována pomocí všech tří představených produktů. Jelikož je rychlost synchronizace dat v podstatě neporovnatelnou veličinou, která je závislá na mnoha faktorech, bude vybráno jednotné úložiště, kterým je populární Google Drive.

Zařízení, na kterém bude probíhat analýza je pouze jeden běžný notebook s níže uvedenými základními parametry, aby nedošlo ke zkreslení závěrů, ke kterému by mohlo dojít střídáním různých zařízení.

- operační systém: Windows 7 SP1 build 7601 (64bitová verze)
- procesor: Intel Core i5 2430M (2,40 GHz)
- operační paměť: 8 GB
- diskové jednotky typu HDD i SSD

7.3 Postup činností práce

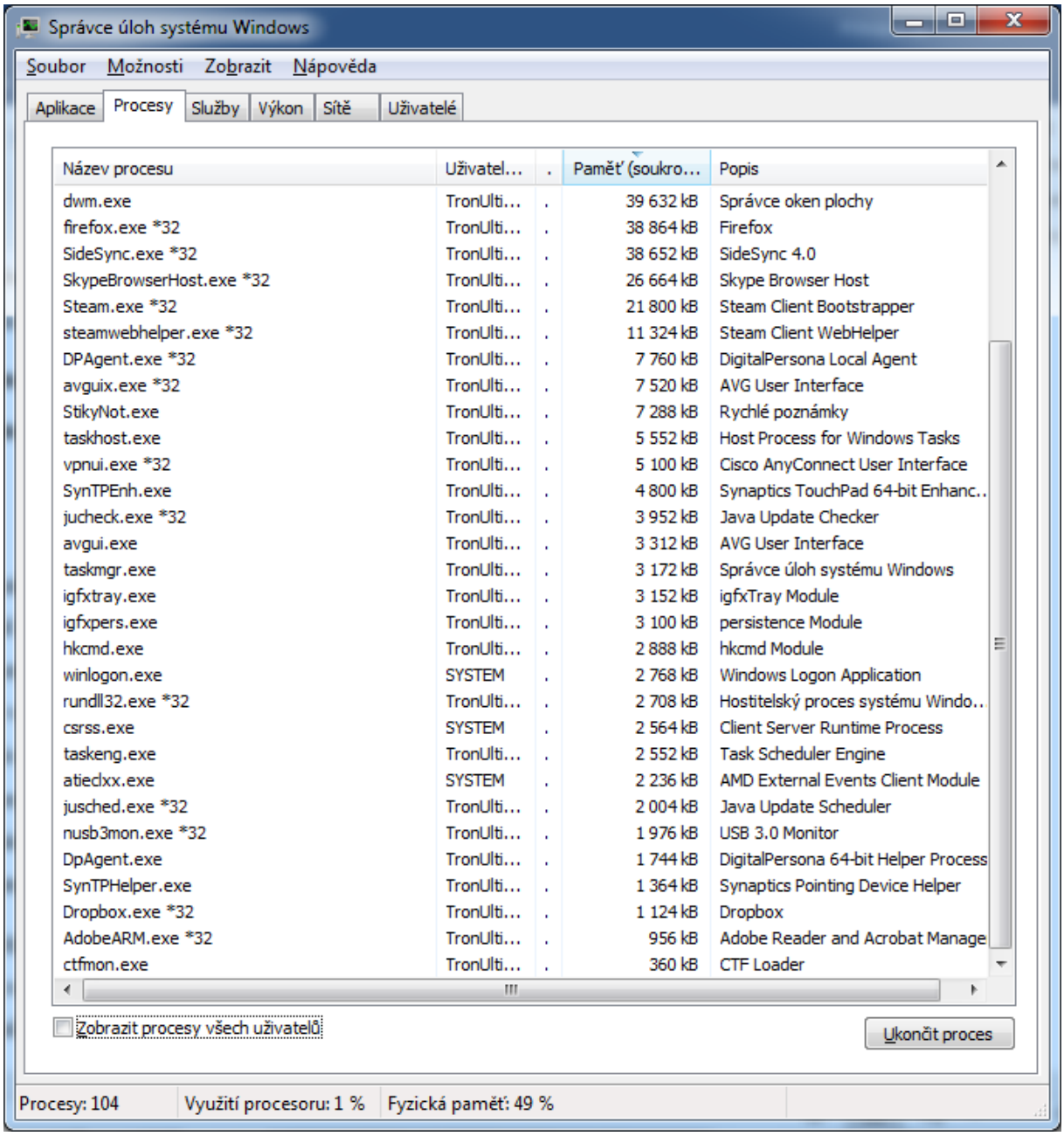
Před samotným zahájením testování bylo nutné vybrat vhodný software pro sledování využití systémových prostředků. S výhodou je možné použít nástroj pojmenovaný Sledování výkonu, který je součástí systému Windows 7. Tento nástroj poskytuje rozsáhlé možnosti sledování systému. V následující analýze bude sledováno využití procesoru a operační paměti při procesu šifrování dat na cloud pomocí dříve popsaných nástrojů.

Prvním krokem bylo vygenerování testovacích dat. Generování proběhlo pomocí volně dostupného nástroje File Generator (verze 3.6.0), který je součástí balíku systémových nástrojů, staženého ze stránek produktu [25]. Generováno bylo 10000 souborů, z nichž každý má velikost 4096 B a jeden soubor o velikosti 1024 MB. Následuje analýza využití prostředků počítače jednotlivými nástroji při činnosti šifrování a synchronizace nejdříve většího množství menších souborů, poté jednoho objemného a následná reprezentace výsledků. Zvolený interval snímání dat je 1 sekunda.

7.4 Popis měření

Měření probíhalo navázáním sledovacího nástroje na procesy jednotlivých produktů. Bylo spuštěno těsně před zahájením celého procesu a ukončeno ihned po skončení šifrovacího procesu, protože samotné dokončení synchronizace může být v závislosti na rychlosti internetového připojení časově náročné. Vzhledem k faktu, že se primární sledování týká šifrování, tak pro srovnávací účely využití prostředků je toto kritérium dostačující. Ani jeden z programů nenabízí možnost změny délky šifrovacího klíče, a s tím spojené úrovně šifrování. U všech tří nástrojů probíhaly veškeré činnosti v adresáři úložiště Google Drive, a tudíž zde může nastat latence způsobená odesíláním dat na server.

Měření probíhalo při běžném provozu počítače, a tak byly systémové prostředky vytěžovány také ostatními procesy, což částečně simuluje uživatelské využitích těchto šifrovacích nástrojů. Režim spotřeby energie nebyl nijak regulován. Následuje část orientačního výpisu obvykle spuštěných uživatelských procesů v pozadí.



Obrázek 3 - Výpis běžících procesů

Ze snímku je patrné, že ač je momentální úroveň využití procesoru nízká, tak lze předpokládat zahájení činnosti některého z nich, zvýšení vytížení prostředků, a s tím spojené ovlivnění rychlosti šifrovacího procesu.

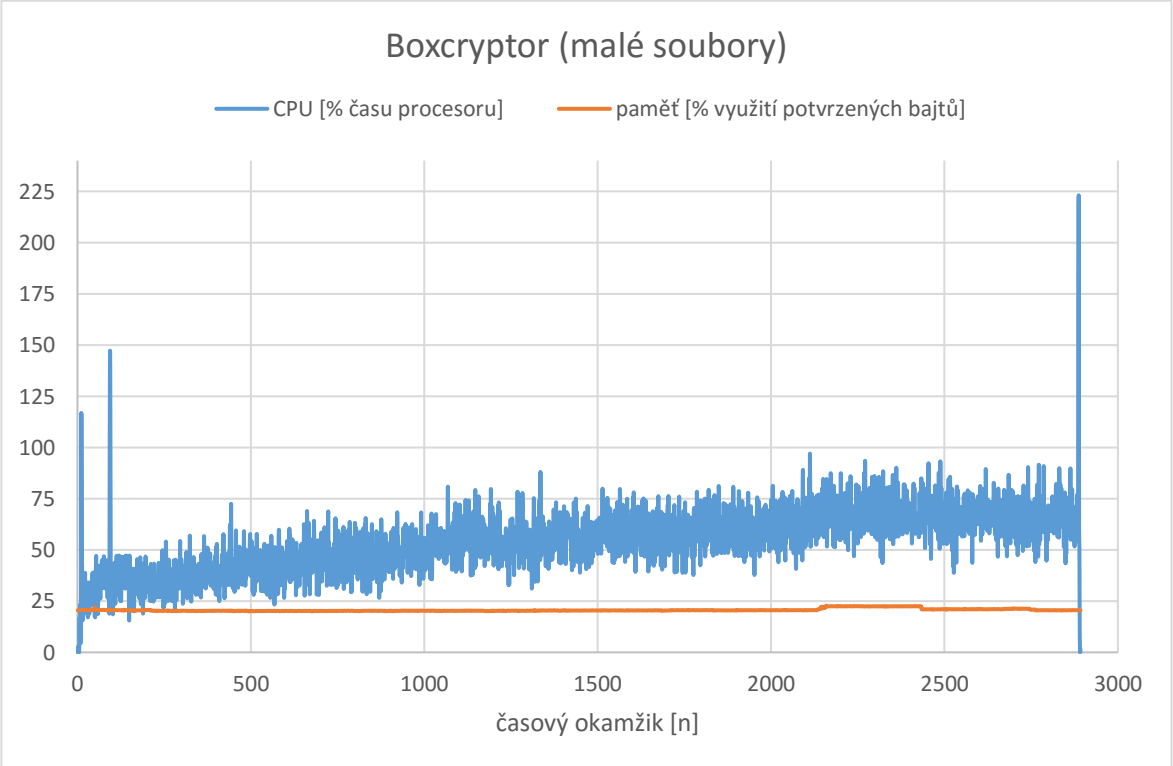
7.5 Boxcryptor

Prvním krokem byla instalace programu (verze 2.12.553), staženého z webových stránek nástroje [20]. Dále byla nutná registrace a aktivace Boxcryptor účtu a převzetí zodpovědnosti za zapamatování svého hesla. Poté proběhl výběr varianty, která je v tomto případě základní bezplatnou verzí. Posledním krokem je přihlášení do klientské aplikace, přidělení práv ke čtení z Google Drive a následný stručný návod k používání.

Program dále vytvořil virtuální diskovou jednotku s písmenem X, do které se připojil adresář Google Drive. V tomto adresáři pak v kontextové nabídce souboru přibyla kolonka Boxcryptor, kde je k dispozici mj. možnost Encrypt (šifrovat), a poté případně Decrypt (dešifrovat) a další. Jednoduché kliknutí na tlačítko Encrypt spustí proces šifrování a synchronizace zašifrovaných dat na úložiště. Možností je také automatické šifrování. Bylo zjištěno, že Boxcryptor soubory šifruje „na cestě“, tudíž není nutné pro práci s nimi provádět dešifrovací proces [23].

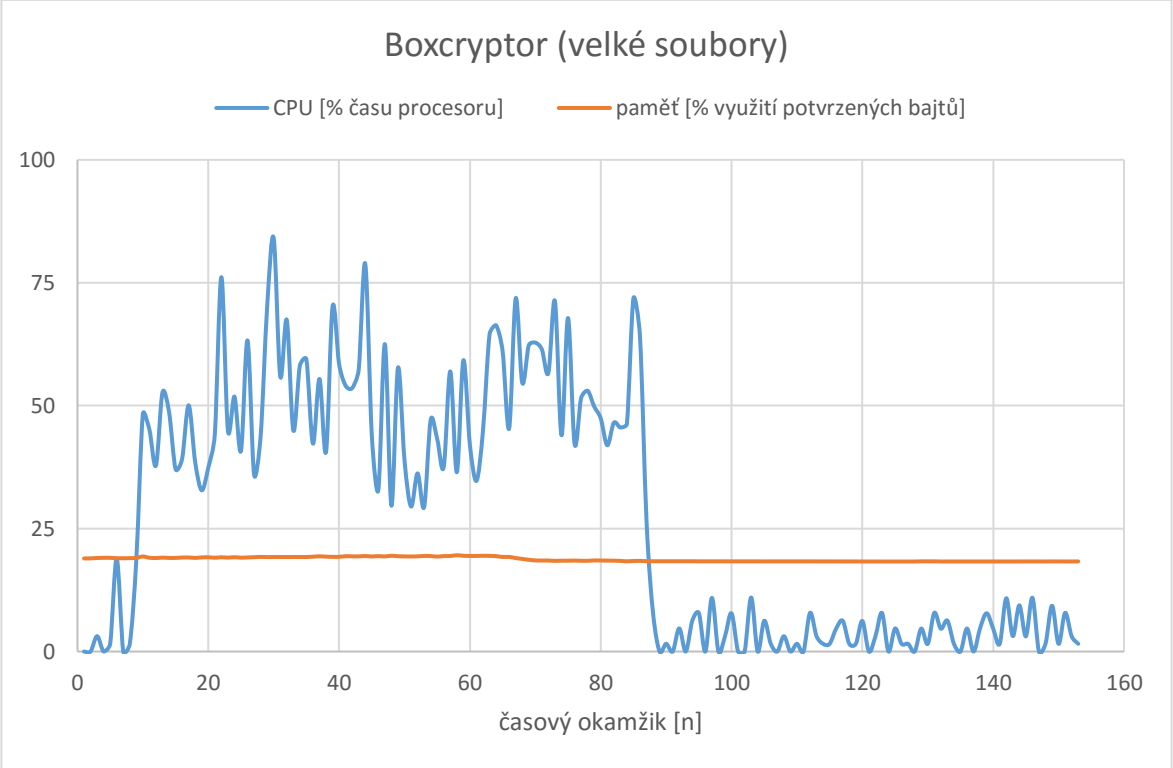
Níže jsou reprezentovány výsledky měření vytížení při používání tohoto programu.

Šifrování velkého množství menších souborů



Obrázek 4 - Graf zatížení systému nástrojem Boxcryptor při šifrování většího množství malých souborů

Šifrování jednoho většího souboru

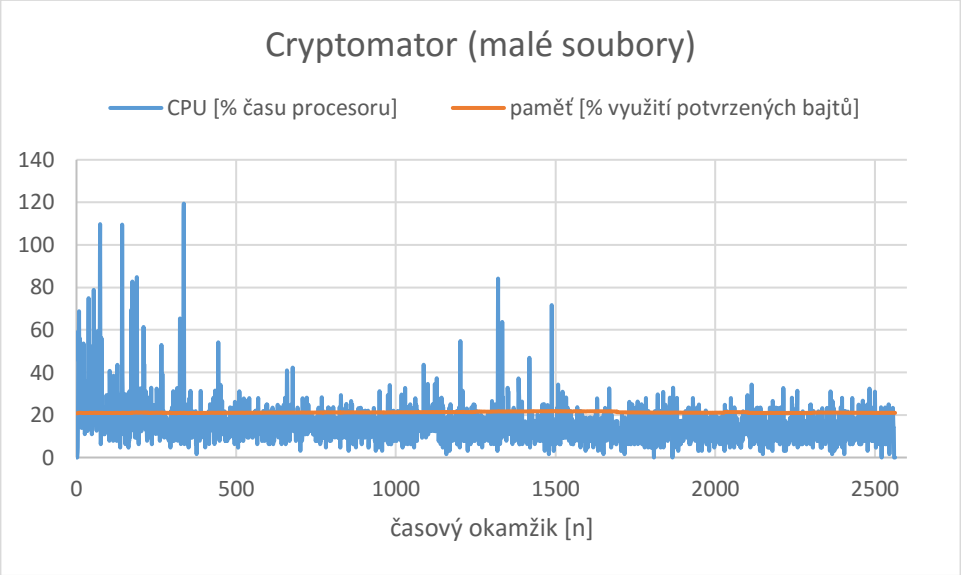


Obrázek 5 - Graf zatížení systému nástrojem Boxcryptor při šifrování jednoho velkého souboru

7.6 Cryptomator

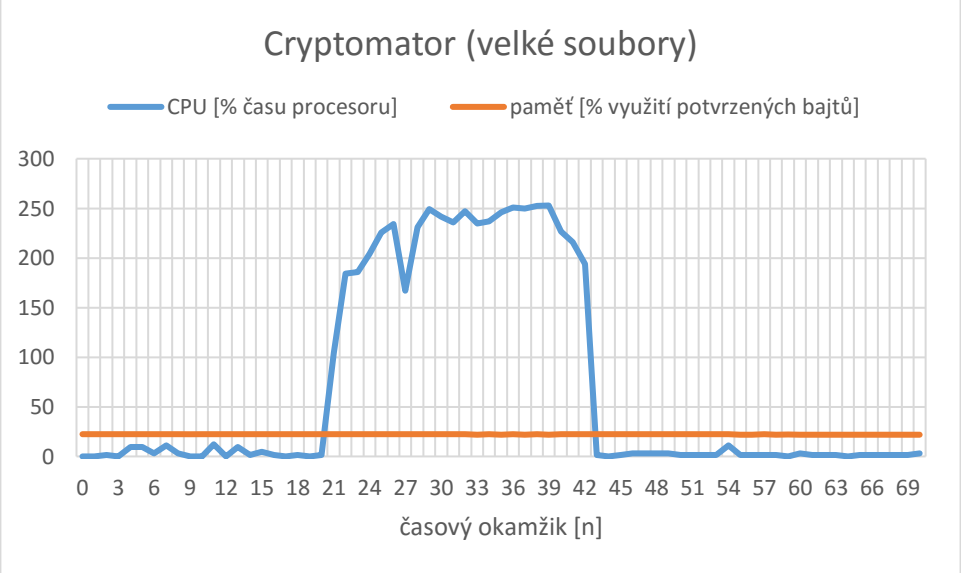
Stejně jako v předchozím případě, nejdříve proběhlo stažení a instalace 64bitové verze programu (verze 1.2.3), který byl získán na webu produktu [21]. Průběh instalace nebyl ničím výjimečný a produkt byl nainstalován během několika vteřin. Dalším krokem bylo vytvoření tzv. trezoru, což je datová jednotka, kterou využívá program jako kontejner pro šifrovaná data. Vzhledem k charakteru využití nástroje, je vhodné vybrat adresář datového úložiště, na kterém chceme data šifrovat. Program při vytváření trezoru požádá o heslo ke kontejneru, prostřednictvím kterého lze pak s daty v kontejneru pracovat. Trezor se poté snadno pouze odemyká nebo zamyká. Po vytvoření a odemčení trezoru se připojí virtuální disková jednotka, do které se vkládají data, která jsou určena pro zabezpečení. Nakonec stačí trezor zamknout, a tím proces končí.

Šifrování velkého množství menších souborů



Obrázek 6 - Graf zatížení systému nástrojem Cryptomator při šifrování většího množství malých souborů

Šifrování jednoho většího souboru

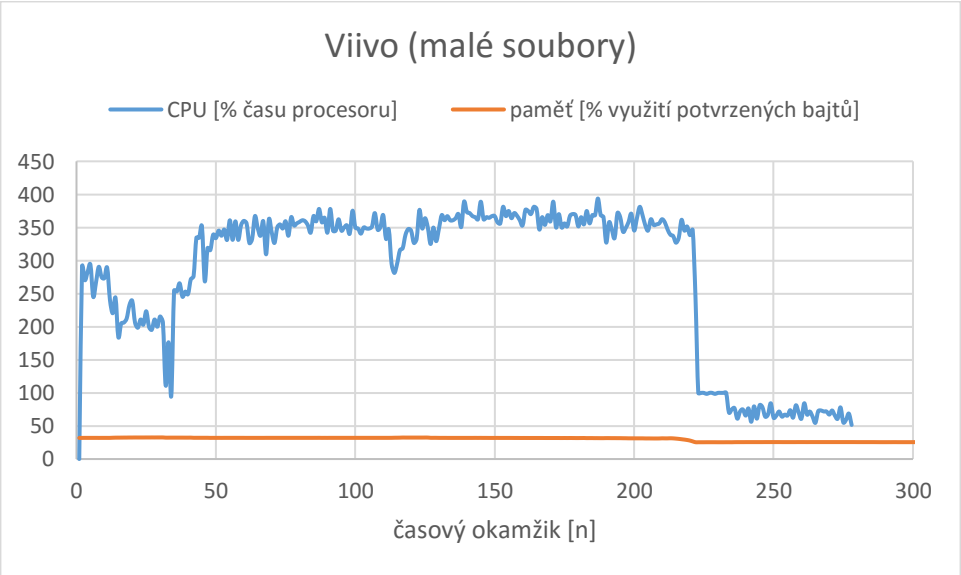


Obrázek 7 - Graf zatížení systému nástrojem Cryptomator při šifrování jednoho většího souboru

7.7 Viivo

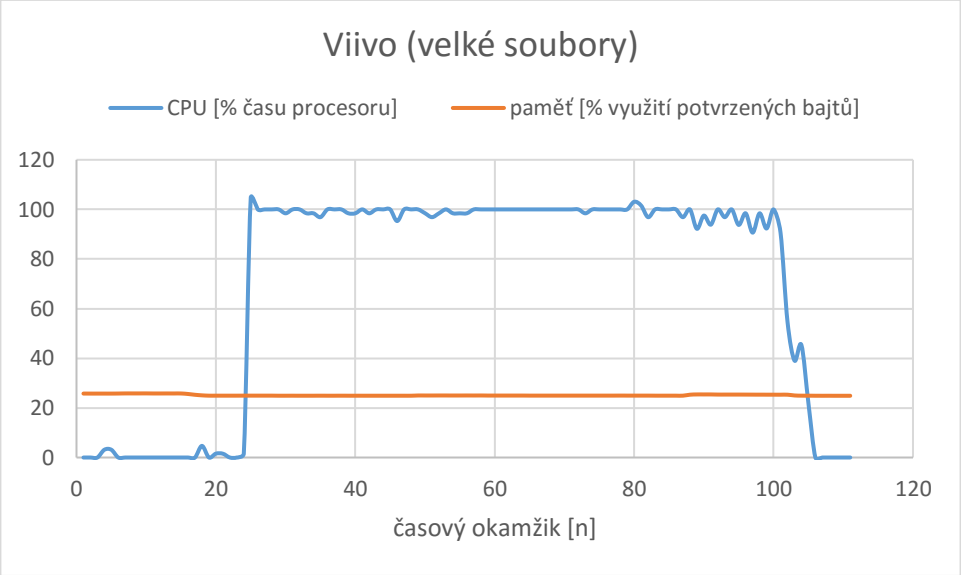
Nejdříve bylo opět nutné stáhnout program (verze 3.0.102) ze stránek produktu [55] a provést instalaci. Po spuštění proběhla, v našem případě, registrace účtu Viivo (jinak stačí přihlášení) a aktivace účtu prostřednictvím odkazu v emailové zprávě. Po aktivaci již bylo možné pokračovat v práci s programem. V první řadě bylo vytvořit tzv. locker (zámek, skříňka), kterému se přiřadí vybraná složka v počítači, kterou je v našem případě vybraný adresář v úložišti Google Drive. Dalším krokem je volba, zda smí Viivo ukládat nezašifrované kopie dat. V případě kladné volby je synchronizace povolena, v opačném případě není (možná pozdější změna). Z uživatelských souborů se stanou soubory s alternativní příponou (.viivo), která jsou poté v závislosti na nastavení úložiště synchronizovány.

Šifrování velkého množství menších souborů



Obrázek 8 - Graf zatížení systému nástrojem Viivo při šifrování většího množství malých souborů

Šifrování jednoho většího souboru



Obrázek 9 - Graf zatížení systému nástrojem Viivo při šifrování jednoho velkého souboru

7.8 Porovnání výsledků

V grafech byla porovnána procentuální vyjádření úrovně využití systémových prostředků vzhledem k časovému okamžiku. Náš zvolený časový okamžik nese označení n a je shodný s frekvencí snímání hodnot vytížení, což je 1 sekunda.

Z výsledků měření jednotlivými produkty jsou zřejmé rozdíly ve využití systémových prostředků a zátěži při procesu šifrování. První dva testované produkty vykázaly přibližně očekávané chování, třetí z nich vykázal chování poměrně abnormální. Byly naměřeny velice nízké hodnoty zatížení převážně procesoru, a to vše ve velmi krátkém čase.

Při testování třetího produktu (Viivo), panoval názor, že měření proběhlo chybně, a proto následovalo opakované měření. Výsledky však byly totožné a hodnoty byly vyneseny do grafu. Neočekávaný výsledek může mít mnoho příčin, a patří mezi ně hlavně kvalita zpracování programu, jiná vnitřní logika nástroje a jeho funkčnost. Vzhledem k faktu, že není možný přístup do programu na takové úrovni, aby bylo možné porovnání způsobu provádění výpočtů, jsou výsledky druhého pokusu měření považovány za akceptované.

8 ZÁVĚR

V této práci proběhla definice samotného cloudu, představení principů fungování cloudu, ukázka několika možností využití a v neposlední řadě také zmínka o historii této myšlenky. Následuje kapitola, která se zabývá parametry cloudových úložišť, včetně přehledu dostupnosti pro uživatele a krátká zmínka o nynějších poskytovatelích vzdálených úložišť.

Na tuto zmínku navazuje obsáhlá kapitola, která obsahuje analýzu a přehled několika nynějších produktů, jejichž hlavním zaměřením je poskytování cloudového úložiště. U každého byla zkoumána cena poskytovaných služeb, podmínky, jejich splnění je nutné pro využívání dané služby, a nakonec stěžejní informace o poskytovaném zabezpečení, které s daným produktem přichází.

Následující kapitola přináší srozumitelný úvod do problematiky šifrování, převážně symetrické a asymetrické šifry, což úzce souvisí s možnostmi šifrování dat na vzdáleném úložišti.

S výhodou na tuto kapitolu navazuje další, ve které proběhla analýza možností zabezpečení dat v cloudu, pomocí nástrojů třetích stran. Průzkumem trhu byly vybrány tři nástroje, u kterých byly sledovány charakteristiky spojené se zabezpečením, šifrováním a dalšími funkcionalitami. Samozřejmostí bylo zjištění požadavků, které musí zařízení uživatele splňovat, v případě, že daný produkt chce využívat. Nakonec jsou uvedeny informace spojené s licencováním a případným zpoplatněním.

Poslední tvůrčí částí práce je praktická komparativní analýza výše zmíněných nástrojů. Proběhla instalace daných produktů, vygenerování testovacích dat a sledování zatížení systémových prostředků při procesu šifrování. Poté byla naměřená data vynesena do grafů pro vizualizaci a následovalo porovnání výsledků.

Jednotlivé části zadání byly dostatečně splněny a veškeré okruhy informací pokryty. Do práce byly taktéž z důvodu kompletnosti přehledu zahrnuty některé vhodně související informace. Čtenář získá při studiu práce ucelené informace a přehled v oblasti cloud computingu se zaměřením na cloudová úložiště.

Z informací a dat, uvedených ve všech analýzách, které byly provedeny lze usoudit, že vzhledem k stále se zvyšujícímu počtu pokusů o krádež dat na všech typech vzdálených úložišť, je použití šifrovacího nástroje velmi vhodným a elegantním řešení, a to vše i za cenu času a vytížení systémových prostředků, které samotné šifrování vyžaduje. Nutno zmínit, že výkon mobilních zařízení, osobních počítačů i větších serverových jednotek exponenciálně roste, z čehož plyne, že se samotný proces zabezpečení dat stává více dostupným a méně náročným pro každého uživatele, správce nebo samotného poskytovatele vybraných služeb. Na závěr je vhodné uvést, stále se zvyšující délka šifrovacích klíčů a kvalita provedení samotných algoritmů zajišťuje, že i při výkonu dnešních počítačů může zabrat pokus o prolomení šifrovacích technik nepředstavitelně velké množství času.

9 SEZNAM POUŽITÉ LITERATURY

1. About Amazon Drive for Desktop. *Amazon.com* [online]. Seattle: Amazon, c1996-2017 [cit. 2017-05-05]. Dostupné z: https://www.amazon.com/gp/help/customer/display.html?nodeId=201601260
2. About the Amazon Drive Mobile App. *Amazon.com* [online]. Seattle: Amazon, c1996-2017 [cit. 2017-05-05]. Dostupné z: https://www.amazon.com/gp/help/customer/display.html?nodeId=201809590
3. About the Amazon Prime Membership Charge. *Amazon.com* [online]. Seattle: Amazon, c1996-2017 [cit. 2017-05-05]. Dostupné z: https://www.amazon.com/gp/help/customer/display.html?nodeId=200966690
4. AES encryption for all cloud storage providers. *Boxcryptor* [online]. Augsburg: Secomba [cit. 2017-05-05]. Dostupné z: https://www.boxcryptor.com/en/providers/
5. Amazon Drive. *Amazon.com* [online]. Seattle: Amazon, c1996-2017 [cit. 2017-05-05]. Dostupné z: https://www.amazon.com/b/?_encoding=UTF8&%2AVersion%2A=1&%2Aentries%2A=0&node=15547130011
6. BAUN, Christian, Marcel KUNZE, Jens NIMIS a Stefan TAI. *Cloud Computing: Web-Based Dynamic IT Services*. 2nd edn. Berlin: Springer-Verlag, 2011. ISBN 978-3-642-20916-1.
7. Best Cloud Storage Services. *Technology reviews, advice, videos, news and forums - PC Advisor* [online]. London: IDG, 2017 [cit. 2017-05-05]. Dostupné z: http://www.pcadvisor.co.uk/test-centre/internet/best-cloud-storage-services-2017-uk-3614269/
8. Best Free Cloud Storage Providers. *Arabia Technology* [online]. Beirut: LCIS, 2016 [cit. 2017-05-05]. Dostupné z: http://arabia.technology/en/archives/2065
9. BOŘÁNEK, Roman. Cryptomator: jednoduché šifrování cloudového úložiště. *Root.cz* [online]. 2017 [cit. 2017-05-05]. ISSN 1212-8309. Dostupné z: https://www.root.cz/clanky/cryptomator-jednoduche-sifrovani-cloudoveho-uloziste/
10. Boxcryptor - Features, Pricing, Alternatives. *PCMag.com* [online]. New York: ZiffDavis, c2016 [cit. 2017-05-05]. Dostupné z: http://www.pcmag.com/business/directory/encryption/1144-boxcryptor
11. Boxcryptor for Individuals. *Boxcryptor* [online]. Augsburg: Secomba [cit. 2017-05-05]. Dostupné z: https://www.boxcryptor.com/en/for-individuals/
12. Boxcryptor for Teams. *Boxcryptor* [online]. Augsburg: Secomba [cit. 2017-05-05]. Dostupné z: https://www.boxcryptor.com/en/for-teams/
13. Ceny tarifů úložiště na iCloudu. *Apple (Česká republika)* [online]. Cupertino: Apple, c2017 [cit. 2017-05-06]. Dostupné z: https://support.apple.com/cs-cz/HT201238
14. *Cloud* [online]. Cupertino: Apple, c2017 [cit. 2017-05-05]. Dostupné z: https://www.icloud.com/
15. Cloud computing: Co ty pojmy znamenají? *Cloud.cz* [online]. [cit. 2017-05-05]. Dostupné z: http://www.cloud.cz/cloud/158-cloud-computingco-ty-pojmy-znamenaji.html
16. Co je to cloud computing? - Správa.sítě.eu. *Správa sítě - slovník pojmů: správa sítě, zabezpečení sítě, outsourcing IT* [online]. Praha: Aira GROUP [cit. 2017-05-05]. Dostupné z: http://www.sprava-site.eu/cloud-computing/
17. *Cryptomator* [online]. Sankt Augustin: Skymatic UG [cit. 2017-05-05]. Dostupné z: https://cryptomator.org/
18. DASGUPTA, Rahul. MEGA vs. Dropbox. *Clour Storage Reviews* [online]. 2016 [cit. 2017-05-06]. Dostupné z: https://cloudstoragereviewed.com/mega-vs-dropbox/
19. DOČEKAL, Daniel. Cloud computing .. je všude okolo nás. *LUPA.cz* [online]. 2010 [cit. 2017-05-06]. ISSN 1213-0702. Dostupné z: https://www.lupa.cz/clanky/cloud-computing-je-vsude-okolo-nas/

20. Download. *Boxcryptor* [online]. Augsburg: Secomba [cit. 2017-05-05]. Dostupné z: https://www.boxcryptor.com/en/download/
21. Downloads. *Cryptomator* [online]. Sankt Augustin: Skymatic UG, 2017 [cit. 2017-05-05]. Dostupné z: https://cryptomator.org/downloads/
22. *Dropbox* [online]. San Francisco: Dropbox [cit. 2017-05-05]. Dostupné z: https://www.dropbox.com/
23. Encrypting and Decrypting - Boxcryptor Windows EN - Boxcryptor Support Center. *Boxcryptor 2.0 Documentation* [online]. Sydney: Atlassian, 2016 [cit. 2017-05-05]. Dostupné z: https://support.boxcryptor.com/display/BCWINEN/4.+Encrypting+and+Decrypting
24. *Encryption software to secure cloud files* [online]. Augsburg: Secomba [cit. 2017-05-05]. Dostupné z: https://www.boxcryptor.com/en/
25. Free Disk Tools software. *Download software tools.*. [online]. 2014 [cit. 2017-05-05]. Dostupné z: http://www.soft.tahionic.com/download-file-generator/index.html#file_generator
26. Google Drive vs Dropbox. *Cloudfind* [online]. Cloudfind, c2016 [cit. 2017-05-06]. Dostupné z: https://cloudfindhq.com/google-drive-vs-dropbox/
27. How data encryption works in OneDrive for Business and SharePoint Online. *Office Blogs* [online]. Redmond: Microsoft, c2017 [cit. 2017-05-05]. Dostupné z: https://blogs.office.com/2015/01/30/data-encryption-works-onedrive-business-sharepoint-online/
28. How do I upload files to MEGA? *MEGA* [online]. MEGA, 2016 [cit. 2017-05-05]. Dostupné z: https://mega.nz/help/client/webclient/getting-started/how-do-i-upload-files-to-mega
29. How much does Dropbox cost? *Dropbox* [online]. San Francisco: Dropbox [cit. 2017-05-05]. Dostupné z: https://www.dropbox.com/help/billing/cost
30. HURWITZ, Judith, Marcia KAUFMAN, Fern HALPER a Daniel KIRSCH. *Hybrid Cloud For Dummies*. 2. ilustrované vydání. Hoboken: Wiley Publishing, 2012. ISBN 9781118235003.
31. HURWITZ, Judith, Robin BLOOR, Marcia KAUFMAN a Fern HALPER. *Cloud Computing For Dummies*. Hoboken: Wiley Publishing, 2010. ISBN 978-0-470-48470-8.
32. LUKEŠ, Jindřich. Stává se z OneDrive nejlepší cloudové úložiště? *WMMania.cz* [online]. Cheb, 2014 [cit. 2017-05-05]. Dostupné z: https://wmmania.cz/clanek/stava-se-z-onedrive-nejlepsi-cloudove-uloziste/
33. MÁCHA, Petr. Historie a základní principy cloud computingu. *IT Systems* [online]. 2015 [cit. 2017-05-05]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/virtualizace/historie-a-zakladni-principy-cloud-computingu.htm
34. *MEGA* [online]. MEGA, c2017 [cit. 2017-05-05]. Dostupné z: https://mega.nz/
35. MEGA Mobilní aplikace. *MEGA* [online]. MEGA, c2017 [cit. 2017-05-05]. Dostupné z: https://mega.nz/mobile
36. MEGA. *MEGA* [online]. MEGA, c2017 [cit. 2017-05-05]. Dostupné z: https://mega.nz/pro
37. MEGA. *MEGA* [online]. MEGA, c2017 [cit. 2017-05-05]. Dostupné z: https://mega.nz/sync
38. MUCHMORE, Michael a Jill DUFFY. Google Drive Review & Rating. *PC Magazine* [online]. 2016 [cit. 2017-05-05]. ISSN 0888-8507. Dostupné z: http://www.pcmag.com/article2/0,2817,2403546,00.asp
39. OneDrive system requirements - OneDrive. *Microsoft* [online]. Redmond: Microsoft, c2017 [cit. 2017-05-05]. Dostupné z: https://support.office.com/en-us/article/OneDrive-system-requirements-cc0cb2b8-f446-445c-9b52-d3c2627d681e
40. PREECE, Jeph. Amazon Cloud Drive Review. *Top Ten Reviews* [online]. 2017 [cit. 2017-05-05]. Dostupné z: http://www.toptenreviews.com/services/internet/best-online-storage-services/amazon-cloud-drive-review/
41. PREECE, Jeph. Microsoft OneDrive Review. *Top Ten Reviews* [online]. 2017 [cit. 2017-05-05]. Dostupné z: http://www.toptenreviews.com/services/internet/best-online-storage-services/microsoft-onedrive-review/

42. Security Architecture. *Cryptomator* [online]. Sankt Augustin: Skymatic UG [cit. 2017-05-05]. Dostupné z: https://cryptomator.org/architecture/
43. SETÍKOVSKÁ, Blanka. *Cloud Computing*. Praha, 2010. Diplomová práce. České vysoké učení technické v Praze, Fakulta elektrotechnická.
44. System requirements and browsers. *Google* [online]. Mountain View: Google, c2017 [cit. 2017-05-05]. Dostupné z: https://support.google.com/docs/answer/2375082?co=GENIE.Platform%3D
45. System requirements for iCloud. *Apple* [online]. Cupertino: Apple, c2017 [cit. 2017-05-05]. Dostupné z: https://support.apple.com/en-us/HT204230
46. System requirements to run Dropbox. *Dropbox* [online]. San Francisco: Dropbox [cit. 2017-05-05]. Dostupné z: https://www.dropbox.com/help/desktop-web/system-requirements
47. Šifrování dat. *Bezpečný internet* [online]. [cit. 2017-05-05]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-dat/sifrovani-dat.aspx
48. Šifrování, digitální podpis, certifikát, certifikační autorita a další pojmy. *Katedra fyziky PřF UJEP* [online]. Praha, c2001 [cit. 2017-05-05]. Dostupné z: http://physics.ujep.cz/~mskoumal/school/semi/dig_key/teorie.html
49. Tarify/plány pro Microsoft OneDrive. *Microsoft OneDrive* [online]. Redmond: Microsoft, c2017 [cit. 2017-05-05]. Dostupné z: https://onedrive.live.com/about/cs-CZ/plans/
50. Technical Overview. *Boxcryptor* [online]. Augsburg: Secomba [cit. 2017-05-05]. Dostupné z: https://www.boxcryptor.com/en/technical-overview/
51. Technická specifikace. *WEDOS DISK* [online]. Hluboká nad Vltavou: WEDOS Internet, c2017 [cit. 2017-05-05]. Dostupné z: https://disk.wedos.com/cs/technicka-specifikace.html
52. Úložiště na Disku. *Google* [online]. Mountain View: Google, c2017 [cit. 2017-05-05]. Dostupné z: https://www.google.com/settings/storage
53. Upgrade. *Viivo* [online]. Milwaukee: PKWARE, c2016 [cit. 2017-05-05]. Dostupné z: https://www.viivo.com/upgrade
54. Upload or Search for a File or Folder Using the Amazon Drive Website. *Amazon.com* [online]. Seattle: Amazon, c1996-2017 [cit. 2017-05-05]. Dostupné z: https://www.amazon.com/gp/help/customer/display.html?nodeId=201376650
55. *Viivo* [online]. Milwaukee: PKWARE, c2016 [cit. 2017-05-05]. Dostupné z: https://viivo.com/
56. WEDOS Disk - základní informace. *Hosting WEDOS* [online]. Hluboká nad Vltavou: WEDOS Internet, c2017 [cit. 2017-05-05]. Dostupné z: https://kb.wedos.com/cs/disk/info.html
57. *WEDOS DISK* [online]. Hluboká nad Vltavou: WEDOS Internet, c2017 [cit. 2017-05-05]. Dostupné z: https://disk.wedos.com/cs/
58. What browser should I use? *MEGA* [online]. MEGA, 2016 [cit. 2017-05-05]. Dostupné z: https://mega.nz/help/client/webclient/general/what-browser-should-i-use
59. What is cloud computing? - Cloud computing news. *IBM - United States* [online]. Armonk: IBM, 2014 [cit. 2017-05-05]. Dostupné z: https://www.ibm.com/blogs/cloud-computing/2014/03/what-is-cloud-computing-2/
60. What is Cloud Computing? - Definition from Techopedia. *Techopedia - Where IT and Business Meet* [online]. Edmonton: Techopedia [cit. 2017-05-05]. Dostupné z: https://www.techopedia.com/definition/2/cloud-computing
61. WINDER, Davey. How secure are Dropbox, Microsoft OneDrive, Google Drive and Apple iCloud cloud storage services? *Aplhr* [online]. 2016 [cit. 2017-05-05]. Dostupné z: http://www.alphr.com/apple/1000326/how-secure-are-dropbox-microsoft-onedrive-google-drive-and-apple-icloud-cloud-storage

PŘÍLOHY

Příloha A – Disk CD

Příloha A – *Disk CD*

OBSAH PŘILOŽENÉHO DISKU CD

1. Vlastní text práce v PDF