

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

WEBOVSKÉ ROZHRANIE PRE BEZPEČNÉ
ZDIELANIE DOKUMENTOV V CLOUDE
BAKALÁRSKA PRÁCA

2015

Peter Kovács

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

WEBOVSKÉ ROZHRANIE PRE BEZPEČNÉ
ZDIEĽANIE DOKUMENTOV V CLOUDE
BAKALÁRSKA PRÁCA

Študijný program: Informatika
Študijný odbor: 2508 Informatika
Školiace pracovisko: Katedra informatiky
Školiteľ: RNDr. Michal Rjaško, PhD.

Bratislava, 2015
Peter Kovács



Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta:

Študijný program: informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)

Študijný odbor: 9.2.1. informatika

Typ záverečnej práce: bakalárska

Jazyk záverečnej práce: slovenský

Názov:

Cieľ:

Literatúra:

**Kľúčové
slová:**

Vedúci:

Katedra: FMFI.KI - Katedra informatiky

Vedúci katedry: doc. RNDr. Daniel Olejár, PhD.

Dátum zadania:

Dátum schválenia:

doc. RNDr. Daniel Olejár, PhD.
garant študijného programu

študent

vedúci práce

Pod'akovanie:

Abstrakt

Slovenský abstrakt 100-500 slov

Kľúčové slová: jedno, druhé, tretie (prípadne štvrté, piate)

Abstract

English abstract

Keywords:

Obsah

Úvod	1
1 Kryptografia	2
1.1 Kryptografia	2
1.2 Množiny a operácie	3
1.3 Symetrické šifrovanie	4
1.4 Asymetrické šifrovanie	4
1.5 Hašhovaciele funkcie	5
1.6 Použité šifry	5
2 Súčasné riešenia	6
2.1 Cloudové úložiská	6
2.2 Existujúce riešenia na šifrované ukladanie dát	6
2.3 Cieľ práce	8
2.4 Porovnanie	8
3 Návrh funkcionality	10
3.1 Prerekvizity	10
3.2 Predpríprava	10
3.3 Nahrávanie dát	11
3.4 Sťahovanie dát	11
3.5 Zdieľanie	11
3.6 Zrušenie zdieľania	11

<i>OBSAH</i>	v
--------------	---

4 Implementacia	12
4.1 Použité technologie	12
4.1.1 Tech1	12
4.1.2 tech 2	12
4.2 Popis riesenia	12
4.2.1 Nejaké veci	12
Záver	13

Zoznam obrázkov

Úvod

Úvod je prvou komplexnou informáciou o práci, jej celi, obsahu a štruktúre. Úvod sa vzťahuje na spracovanú tému konkrétne, obsahuje stručný a výstižný opis problematiky, charakterizuje stav poznania alebo praxe v oblasti, ktorá je predmetom školského diela a oboznamuje s významom, cieľmi a zámermi školského diela. Autor v úvode zdôrazňuje, prečo je práca dôležitá a prečo sa rozhodol spracovať danú tému. Úvod ako názov kapitoly sa nečísluje a jeho rozsah je spravidla 1 až 2 strany.

Kapitola 1

Kryptografia

Prvá kapitola slúži ako teoretický úvod do kryptografie. Vymenujeme jej ciele, zdefinujeme základné pojmy a vysvetlíme, čo je symetrické a asymetrické šifrovanie a ako fungujú. Budeme vychádzať z knihy Handbook of Applied Cryptography [1].

1.1 Kryptografia

Kryptografia sa zaoberá metódami ukladania a prenášania dát vo forme, ktorú dokáže spracovať iba taká entita, ktorej sú dáta určené.

Ciele kryptografie

Na úvod popíšeme základné kryptografické ciele ako dôvernosť, integritu a autentickosť. Z cieľov vynecháme dostupnosť, ktorú kryptografia ako taká nedokáže zabezpečiť.

- Dôvernosť je vlastnosť, ktorá nám zaručuje, že k dátam sa dostanú len také entity, ktorým bola správa určená a nikto iný. Dôvernosť dát budeme zabezpečovať šifrovaním.
- Integrita je vlastnosť, ktorá hovorí o modifikácii dát. Aby sme zaručili

integritu dát, musí byť zaručená možnosť detegovať manipuláciu s dátami neoprávnenými entitami.

- Autentickosť je vlastnosť, ktorá hovorí o pôvode entity alebo dát. Teda keď Anička pošle správu Bohušovi, Bohuš bude môcť overiť, že správa je skutočne od Aničky.

1.2 Množiny a operácie

Zadefinujeme si základné množiny a operácie nad nimi, ktoré budeme používať.

- Množinu \mathcal{A} budeme nazývať abecedou. Abecedou je napríklad slovenská abeceda alebo $\mathcal{A} = \{0, 1\}$ je binárnou abecedou.
- Množina \mathcal{M} je množina všetkých možných správ nad danou abecedou \mathcal{A} . Napríklad nad abecedou $\mathcal{A} = \{0, 1\}$ pri správach maximálnej dĺžky 2 je $\mathcal{M} = \{00, 01, 10, 11\}$.
- Množina \mathcal{C} obsahuje všetky šifrované správy nad danou abecedou \mathcal{A} .
- Množinu \mathcal{K} nazveme množina kľúčov. Prvok $k \in \mathcal{K}$ nazveme kľúč.
- Každý prvok $e \in \mathcal{K}$ jednoznačne určuje bijekciu z \mathcal{M} do \mathcal{C} . Túto transformáciu budeme značiť E_e a budeme ju nazývať šifrovacou funkciou.
- Nech D_d je bijektívna transformácia z \mathcal{C} do \mathcal{M} pomocou prvku $d \in \mathcal{K}$, potom D_d nazveme dešifrovacou funkciou.
- Keď aplikujeme transformáciu E_e na správu $m \in \mathcal{M}$ budeme hovoriť, že šifrujeme správu m . Pokiaľ aplikujeme D_d na $c \in \mathcal{C}$ budeme hovoriť o dešifrovaní.
- Šifra alebo aj šifrovacia schéma sa skladá z množiny $\{E_e : e \in K\}$ a množiny $\{D_d : d \in K\}$, kde platí, že pre každé $e \in K$ existuje $d \in K$ také, že $D_d = E_e^{-1}$ a teda platí aj $D_d(E_e(m)) = m$ pre všetky $m \in \mathcal{M}$.

1.3 Symetrické šifrovanie

Nech šifrovacia schéma pozostáva z množín $\{E_e : e \in K\}$ a $\{D_d : d \in K\}$ kde K je množina všetkých kľúčov. Takúto schému nazveme symetrickou pokiaľ pre každý pár (e, d) platí, že je "ľahké", vypočítať d pomocou e , a opačne. Najčastejšie používame $e = d$. Symetrické šifry sú zväčša veľmi rýchle, takže dokážu zašifrovať veľa dát za krátky čas a taktiež kľúče sú relatívne krátke. Symetrické šifry môžu byť zapúzdrené, teda na jednu správu môže byť použitých viac šifier, vďaka čomu môžu dosahovať väčšiu mieru bezpečnosti. Na druhú stranu pri komunikácii dvoch entít býva dobrým zvykom meniť kľúče relatívne často a taktiež kľúč musí ostať v bezpečí počas celej komunikácie.

1.4 Asymetrické šifrovanie

Nech $\{E_e : e \in K\}$ je množina šifrovacích funkcií a nech $\{D_d : d \in K\}$ je množina príslušných dešifrovacích funkcií a K je množina všetkých kľúčov. Nech pre každý pár (E_e, D_d) platí, že je výpočtovo "nemožné" získať správu $m \in \mathcal{M}$ pomocou $c \in C$ a E_e , keď platí $E_e(m) = c$.

Definícia nám hovorí, že keď máme $e \in K$ tak je nemožné získať príslušný kľúč d taký aby platilo $D_d(E_e(m)) = m$. Aby bola táto vlastnosť zabezpečená, kryptografické funkcie sú založené na matematických problémoch ako je faktorizácia alebo výpočet diskretného logaritmu. Kľúč d budeme nazývať privátnym a e verejným kľúčom. Pri využití asymetrickej kryptografie nám stačí uchovávať privátny kľúč a taktiež kľúče netreba meniť tak často ako pri symetrických šifrách. Nevýhodou oproti symetrickému šifrovaniu môže byť veľkosť kľúčov a rýchlosť šifrovania ktorá býva často nižšia.

1.5 Hašovacie funkcie

Hašovacou funkciou nazveme funkciu ktorá k vstupu ľubovolnej dĺžky vráti reťazec bitov pevnej dĺžky. Jej výstup budeme nazývať haš. Formálnejšie $H : I \rightarrow O$ hašovacou funkciou H nazveme funkciu zobrazujúcu z množiny vstupov I na množinu hašov O . Pre rovnaký vstup bude výstup vždy rovnaký.

Väčšina kryptografických schém využívajúcich hašovacie funkcie využíva takzvané kryptografické hašovacie funkcie. Kryptografická hašovacia funkcia obvykle spĺňa nasledujúce vlastnosti:

1. Jednosmernosť: k danému hašu $o \in O$ je výpočtovo "nemožné" získať akýkoľvek vstup $i \in I$ spĺňajúci $H(i) = o$.
2. Odolnosť voči kolíziám: je výpočtovo "nemožné" nájsť dva rôzne vstupy s rovnakým hašom $i_1 \neq i_2$, kde $i_1, i_2 \in I$ pre ktoré platí, že $H(i_1) = H(i_2)$.

Kryptografické využitie je napríklad v digitálnych podpisoch, konštrukciách autentizačných kódov, pri ukladaní hesiel alebo taktiež môžu slúžiť na kontrolu integrity údajov.

1.6 Použité šifry

AES

Ako moc to mam popisovat??

ECC

Co popisat k tomuto??

Kapitola 2

SúčasnÉ riešenia

V nasledujúcej kapitole popíšeme čo sú vlastne cloudové úložiská, poskytneme prehľad existujúcich riešení šifrovaných úložísk. Uvedieme ich poskytovné služby a spôsob, akým fungujú. V závere kapitoly ich porovnáme s naším riešením.

2.1 Cloudové úložiská

Cloudové úložisko je služba ktorá nám umožňuje manipulovať s priestorom ktorý sme si prenajali od poskytovateľa služby. Táto služba by sa mala byť škálovateľná, vieme jednoducho zväčšiť priestor za ktorý platíme, starať o to aby naše dáta boli stále prístupné čo zahŕňa ochranu voči strate a poškodeniu dát poprípade výpadkom siete.

2.2 Existujúce riešenia na šifrované ukladanie dát

SúčasnÉ služby môžeme rozdeliť do dvoch kategórií. Väčšina z nich poskytuje natívnu aplikáciu do počítača alebo mobilného zariadenia, tá menšia skupina sa zamerala na tvorbu webovej aplikácie, prostredníctvom ktorej užívateľ

spravuje svoje dáta. Šifrovanie prebieha na strane klienta pred prenosom dát do cloud. Väčšina služieb sa snaží dodržiavať zásadu "zero-knowledge", ktorá zaručuje užívateľovi, že poskytovateľ cloudového úložiska nebude mať o jeho dátach nijaké informácie.

Vlastné cloudové riešenie

Jeden z najznámejších poskytovateľov šifrovaného cloudového úložiska je Mega [2]. Okrem webovskej aplikácie ponúka mobilné aj desktopové aplikácie, ktoré môžu niektorí užívatelia preferovať pred webovým rozhraním. Pri ukladaní súborov alebo zložiek Mega vygeneruje náhodný 128-bitový kľúč a následne dáta zašifruje šifrou AES-128. Všetky kľúče sú dostupné pomocou univerzálneho hesla, ktoré sme si zvolili pri registrácii. To je zahašované kryptografickou hašovacou funkciou a uložené na serveroch. Celé šifrovanie prebieha na počítači klienta, takže Mega nemá žiadne informácie o obsahu uloženom v cloude a nepozná naše heslo. Pri zdieľaní súborov sa používa 2048 RSA kľúčový pár pričom jeho univerzálna časť je zašifrovaná univerzálnym kľúčom. Služba ponúka 50 GB zdarma a za 500 GB používateľ zaplatí 9,99\$.

Služby SpiderOak [6] a Wuala [5] tiež využívajú vlastný cloud, ale neposkytujú webové rozhranie a všetky operácie musíme robiť pomocou aplikácie na našom počítači. SpiderOak pracuje na podobných princípoch ako Mega ale namiesto AES-128 používa AES-256. Zadarmo sú dostupné 2 GB úložného priestoru a za 12\$ mesačne je možné ho rozšíriť na 1 TB.

Wuala využíva systém Cryptree [7] v ktorom používa AES-256 na šifrovanie, RSA 2048 na podpisy a zdieľanie dát a SHA-256 na zabezpečenie integrity. Cena sa pohybuje od 0,99 € za 5 GB do 159,90 € za 2 TB.

Všetky tri služby podporujú Windows, Mac, Linux, Android a iOS.

Využívanie dostupných cloudových riešení

Viivo [3] na rozdiel od Megy využíva už existujúce cloudové riešenia, ktoré poskytujú API na prácu so súbormi a vybudoval tak vrstvu medzi klientom a jeho obľúbeným cloudovými úložiskami Drive, Dropbox, Box alebo SkyDrive.

Viivo vytvorí 2048 bitový kľúčový pár, ktorý sa používa pri zdieľaní dát. Kľúč je zabezpečený pomocou hesla, ktoré si užívateľ zvolí pri registrácii. Pre súkromné využitie je zadarmo, firmy si priplatia od 4,99 do 9,99 mesačne.

Boxcryptor [4] je ďalšia služba podobná Viivu, ktorá vytvorila vrstvu medzi cloudom a používateľom. Podporuje rovnaké cloudy ako Viivo a navyše ešte SugarSync. Kryptografia funguje na rovnakých princípoch ako Mega, ale využíva silnejšie kľúče, t.j. AES-256 pri symetrickej a RSA s kľúčom dĺžky 4096 bitov pri asymetrickej kryptografii. Základné šifrovanie je poskytované zadarmo, neobmedzený firemný účet stojí 96\$ ročne.

Viivo ani Boxcryptor neposkytujú webové rozhranie, takže používateľ je nútený inštalovať dodatočný softvér ktorý je kompatibilný s Windowsom, Macom ako aj s iOSom a Androidom.

2.3 Ciel' práce

Pre naše riešenie sme sa rozhodli skombinovať dva prístupy. Rozhodli sme sa používať už existujúce cloudové úložiská ku ktorým vytvoríme webové rozhranie. Netreba ho inštalovať, čo zvyšuje použiteľnosť a podporuje okrem počítačov aj mobilné zariadenia. Keby sme sa rozhodli pre natívnu aplikáciu, nielen že by sme potrebovali naprogramovať aj mobilný variant, ale aj by sme zaťažovali cieľového užívateľa sťahovaním a inštalovaním. Preto sme vytvorili jednoduché a prehľadné prostredie, z ktorého bude možné využívať viacero úložísk. Pre testovanie a koncept návrhu budeme využívať cloudové úložisko firmy Google, Drive. Našu službu sme sa rozhodli nazvať SecureCloud.

2.4 Porovnanie

V tejto časti vysvetlíme, v čom sa bude SecureCloud líšiť od ostatných služieb a aká je naša motivácia vytvoriť vlastné riešenie.

Mega vs SecureCloud

Mega patrí medzi najlepších poskytovateľov šifrovaných cloudových riešení na trhu. Bohužiaľ veľa ľudí nechce začať využívať iné riešenie ako to, na aké boli doteraz zvyknutí. Medzi najpoužívanejšie a najznámejšie rozhodne patrí Google-Drive a Dropbox, ale ani jedno neponúka šifrovanie dát. Výhoda SecureCloudoproti Mega spočíva v možnosti pokračovať vo využívaní služieb Googlu alebo Dropboxu a zároveň v zabezpečení šifrovania dát. Modelový užívateľ, ktorý uprednostní naše riešenie oproti riešeniu Megy, je taký, ktorý má napríklad zaplatený poplatok za priestor u jedného zo spomenutých prevádzkovateľov.

Viivo a Boxcryptor vs SecureCloud

Napriek tomu, že Viivo aj Boxcryptor ponúkajú využívanie vrstvy medzi obľúbenými poskytovateľmi úložísk a používateľom, nemajú nijaké webové rozhranie, čo zaťažuje používateľa okrem registrácie aj inštaláciami mobilných a desktopových aplikácií na všetkých zariadeniach, na ktorých budú službu využívať. Naopak naše riešenie vyžaduje iba prihlásenie pomocou už existujúceho Dropbox alebo Google konta.

Kapitola 3

Návrh funkcionality

Ďalej opíšeme ako sme navrhli naše riešenie. TODO

3.1 Prerekvizity

Aby naše riešenie fungovalo, budeme potrebovať server, ktorý bude slúžiť na hostovanie našej služby, databázu, ktorá bude ukladať užívateľove dáta a cloudové úložisko, ktoré bude zabezpečovať prácu so súbormi. Cloud musí poskytovať rozhranie pomocou ktorého vieme nahrávať a sťahovať dáta a taktiež musí byť schopné autorizovať rôznych užívateľov pre prístup k dátam iných užívateľov, aby sme boli schopný zdieľať súbory s inými používateľmi.

3.2 Predpríprava

Keď sa používateľ rozhodne používať našu službu musí sa nejakým spôsobom identifikovať a autentifikovať. K tomuto poslúži nejaká forma registrácie pri ktorej si užívateľ zvolí svoje univerzálne heslo pomocou ktorého bude autorizovať akcie ako nahrávanie, sťahovanie, zdieľanie a zrušenie zdieľania dát. Následne v užívateľovom prehliadači vygenerujeme verejný a privátny kľúč, ktorý symetricky zašifrujeme pomocou už zvoleného univerzálneho hesla. Verejný aj zašifrovaný privátny kľúč uložíme na servri kde prístup k verejným

klúčom budú mať všetci používatelia no k privátnym len jeho vlastníci. Tým že privátny klúč je zašifrovaný server nemá žiadnu informáciu o privátnom klúči a teda schéma ostane bezpečná.

3.3 Nahrávanie dát

Užívateľ si v prehliadači vygeneruje, pomocou dostatočne náhodného generátoru, náhodné heslo ktorým zašifruje súbor a vypýta si od serveru svoj verejný klúč ktorým heslo zašifruje. V takomto tvare ho môže poslať na server spolu s identifikátorom súboru. Keďže heslo je zašifrované a server nemá informáciu o privátnom klúči užívateľove dáta by mali byť stále v bezpečí. Následne už len stačí zašifrovaný súbor nahrať na cloudové úložisko.

3.4 Sťahovanie dát

3.5 Zdieľanie

3.6 Zrušenie zdieľania

Start

Kapitola 4

Implementacia

V tejto kapitole budem popisovat hlavne implementacne detaily

4.1 Použité technologie

Tu spravim prehľad technologií ktore som pouzil preco som sa rozhodol pouzit toto a nie nieco ine a tak podobne.

4.1.1 Tech1

4.1.2 tech 2

4.2 Popis riesenia

Tu popisem ako funguje moje riesenie.

4.2.1 Nejaké veci

Záver

V závere je potrebné v stručnosti zhrnúť dosiahnuté výsledky vo vzťahu k stanoveným cieľom. Rozsah záveru je minimálne dve strany. Záver ako kapitola sa nečísluje.

Literatúra

- [1] Alfred J. Menezes - Paul C. van Oorschot - Scott A. Vanstone, 1996, Handbook of Applied Cryptography, CRC Press
- [2] Mega, Februar 2015, [online] Dostupné na internete: [;https://mega.co.nz/#doc;](https://mega.co.nz/#doc)
- [3] Viivo, Februar 2015, [online] Dostupné na internete: [;https://viivo.com/;](https://viivo.com/)
- [4] BoxCryptor, Februar 2015, [online] Dostupné na internete: [;https://www.boxcryptor.com/en;](https://www.boxcryptor.com/en)
- [5] Wuala, Februar 2015, [online] Dostupné na internete: [;https://www.wuala.com/en/learn/technology;](https://www.wuala.com/en/learn/technology)
- [6] SpiderOak, Februar 2015, [online] Dostupné na internete: [;https://spideroak.com/;](https://spideroak.com/)
- [7] Grolimund D. - Meisser L. - Schmid S. - Wattenhofer R., Cryptree: A Folder Tree Structure for Cryptographic File Systems, [online] Dostupné na internete: [;http://dcg.ethz.ch/publications/srds06.pdf;](http://dcg.ethz.ch/publications/srds06.pdf)