Univerzita Komenského v Bratislave

Fakulta matematiky, fyziky a informatiky

Webovské rozhranie pre bezpečné zdieľanie 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 Informatka
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: Peter Kovács
Študijný program: informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: 9.2.1. informatika
Typ záverečnej práce: bakalárska
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Webovské rozhranie pre bezpečné zdieľanie dokumentov v cloude

Cieľ: Navrhnúť a naprogramovať web aplikáciu, ktorá umožní používateľom bezpečne zdieľať a ukladať dokumenty v cloude. Aplikácia musí zabezpečiť, aby dokumenty boli uložené na serveri v šifrovanej podobe a server nemal prístup k dokumentom v otvorenom tvare. Zároveň treba navrhnúť praktický spôsob na distribúciu kľúčov k jednotlivým dokumentom medzi používateľmi, spôsob zdieľania šifrovaných dokumentov (resp. kľúčov na dešifrovanie týchto dokumentov) a revokáciu použitých kľúčov. Celá aplikácia bude na klientovi bežať v prostredí internetového prehliadača.

Vedúci: RNDr. Michal Rjaško, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: doc. RNDr. Daniel Olejár, PhD.

Dátum zadania: 23.10.2014

Dátum schválenia: 28.10.2014

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

študent Kovács

Michal Rjaško
vedúci práce

Poďakovanie:

Abstrakt

Slovenský abstrakt 100-500 slov

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

Abstract

English abstract

Keywords:

Obsah

Zoznam obrázkov

Úvod

Úvod je prvou komplexnou informáciou o práci, jej cieli, 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

Súčasné riešenia

V prvej 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.

1.1 Cloudové úložiská

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

1.2 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. 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. Okrem webovskej aplikácie Mega ponúka mobilné aj desktopové aplikácie, ktoré môžu niektorí užívatelia preferovať pred webovým rozhraním. Pri registrácii si zvolíme heslo, ktoré bude použité ako kľúč pri symetrickom šifrovaní našich súborov. Celé šifrovanie prebieha na počítači klienta, takže Mega nemá žiadne informácie o obsahu uloženom v cloude a tiež nepozná naše heslo. Ďalej sú tu služby ako SpiderOak a Wuala, ktoré neposkytujú webové rozhranie a všetky operácie musíme robiť pomocou aplikácie na našom počítači.

Využívanie dostupných cloudových riešení

Viivo 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 cloudovým úložiskom ako napríklad Dropbox, Box alebo SkyDrive. Boxcryptor je ďalšia služba veľmi podobná Viivu, ktorá tiež vytvorila vrstvu medzi cloudom a požívateľom. Viivo ani Boxcryptor neposkytujú webové rozhranie, takže používatel je nútený inštalovať dodatočný software.

1.3 Cieľ práce

Pre naše riešenie sme sa rozhodli skombinovať dva prístupy. Rozhodli sme sa používať už existujúce cloudové úložiská ku ktorým vytvoríme webovské rozhranie. Netreba ho inštalovať, čo zvyšuje pouziteľnosť 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.

1.4 Porovnanie

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

Mega vs SecureCloud

Mega patrí medzi najlepších poskytovateľov šifrovaných cloudových riešení na trhu. Bohužial 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 2

Kryptografia

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

2.1 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.

2.2 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 kazdé $e \in K$ existuje $d \in K$ také, že $E_e = D_d$ a teda platí aj $D_d(E_e(m)) = m$ pre všetky $m \in \mathcal{M}$.

2.3 Symetrické šifrovanie

Nech šifrovacia schéma pozostáva z množín $\{E_e : e \in K\}$ a $\{D_d : d \in K\}$ kde $\mathcal{K}$ 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 vačšiu 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.

2.4 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 $\mathcal{K}$ 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 $e \in \mathcal{K}$ tak je nemožné získat príslušný kľúč d taký aby platilo $D_d(E_e(m)) = m$. Aby sme zabezpečili túto vlastnosť vačšina šifrovacích funkcií je založená na matematických problémoch ako je faktorizácia alebo výpočet diskrétneho 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 velkosť kľúčov a rýchlosť šifrovania ktorá býva často nižšia.

2.5 Vyuzijeme

Tu by sa hodilo popisat nejake šifrovacie veci ktoré budem pouzívať. Napríklad ECC, AES poprípade nejake password derivátory scrypt/bcrypt/pbkdf2 alebo crypto-hash funkcie.

Kapitola 3

Implementacia

V tejto kapitole budem popisovat hlavne implementacne detaily

3.1 Použité technologie

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

3.1.1 Tech1

3.1.2 tech 2

3.2 Popis riesenia

Tu popisem ako funguje moje riesenie.

3.2.1 Nejaké veci

3.3 Zdieľanie súborov

V tejto sekcii popisem ako funguje zdielanie suborov popisme kryptograficku schemu atd.

3.3.1 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