Zdieľanie tajomstva pre správu súkromných údajov

Autor:	Ing. Peter Čuřík
Vedúci práce:	prof. Ing. Pavol Zajac, PhD.
Univerzita:	SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
Fakulta:	FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Táto práca využíva Shamirovu schému zdieľania tajomstva na zvýšenie bezpečnosti pri používaní komerčných cloudov. Výsledkom je aplikácia Datachest, ktorá používateľom umožňuje nahrávanie, sťahovanie a správu svojich citlivých údajov v cloudových úložiskách. Datachest podporuje tri, momentálne širokou verejnosťou, najpoužívanejšie komerčné cloudové úložiská, a to: Google Drive, Microsoft OneDrive a Dropbox. Shamirova schéma je v aplikácii využívaná na rozdeľovanie tajomstva na viacero podielov a na spätné spájanie podielov na získanie pôvodného tajomstva. Je nastavená tak, že tajomstvo sa vždy rozdeľuje na tri podiely, ale na získanie pôvodného tajomstva sú potrebné aspoň dva z troch podielov.

Datachest ukladá používateľom nahrávané súbory na cloud v šifrovanom tvare. Tým pádom je zvýšená dôvernosť uložených údajov. Kľúč (tajomstvo), použitý k šifrovaniu, je rozdelený Shamirovým algoritmom na tri podiely a každý z nich je uložený na iný zo spomenutých troch cloudov. Z definície Shamirovej schémy vieme, že vlastník podielu kľúča má nulovú informáciu o pôvodnom kľúči (tajomstve). Využívame vzájomnú konkurenciu zvolených spoločností (Google, Microsoft, Dropbox) na získanie istoty, že nebudú kolaborovať v záujme získania dostatočného počtu podielov potrebných na získanie pôvodného tajomstva.

Pri sťahovaní šifrovaného súboru je potrebné získať aspoň dva z troch podielov kľúča patriaceho k danému súboru od ostatných cloudov. Podiely sú aplikáciou podľa Shamirovej schémy zlúčené do pôvodného kľúča, ktorým sa šifrovaný súbor pre používateľa dešifruje.

Riešenie tejto práce má potenciál využitia širokou verejnosťou. Aplikácia je efektívna, intuitívna a jednoduchá na používanie. Poskytuje extra úroveň bezpečnosti pri správe údajov v komerčných cloudoch. Podporuje najpoužívanejšie cloudové úložiská. Rieši problém správy kľúčov.