Posudek diplomové práce

Autor: Bc. Lukáš Toman
Název diplomové práce: Vyhledávání nad šifrovanými daty v aplikacích s architekturou klient-server
Posudek vypracoval oponent práce: Ing. Jan Smejkal

Text

Autor se ve své diplomové práci zabývá návrhem, implementací a testováním systému pro vyhledávání nad šifrovanými daty. V úvodu diplomant podrobně vysvětluje základy samotné kryptografie, hlavně principy symetrického a asymetrického šifrování. Následně se text již věnuje analýze požadavků a metod pro vyhledávání nad šifrovanými daty. Text popisující jednotlivé metody je velmi hutný, což považuji za nedostatek práce. Nejsem si jistý, zdali by čtenář bez předchozí znalosti kryptografie jednotlivé metody šifrování a následného vyhledávání pochopil.

Část věnující se výběru jedné z metod je naopak velmi podrobná a zdařilá. Autor zde zároveň navrhuje upravit vybranou metodu tak, aby celkové řešení lépe škálovalo.

Kapitoly zaměřené na návrh architektury a implementaci jsou velmi strohé. Zejména kapitola s názvem implementace popisuje pouze výčet použitých technologií a seznam naimplementovaných modulů. Zde by dle mého názoru bylo vhodné zmínit více detailů týkajících se implementace samotných kryptografických metod (např. jakou knihovnu autor použil.)

Práce podrobněji nepopisuje, jakým způsobem lze knihovnu, která šifruje auditní logy, integrovat do již existujícího systému, kde auditní logy vznikají. Autor sice zmiňuje, že knihovna je implementována jako dll, není zde ale popsán přesný postup, jak by integrace probíhala.

Sekce věnující se testování popisuje řadu postupů, kterými autor ověřil správnost zvolených metod. Množství provedených je více než dostačující.

Po formální stránce je práce psána jednotným stylem. V práci se nenachází žádné velké formální nedostatky.

Implementace

S autorem jsem si domluvil telekonferenci, během které mi odprezentoval jednotlivé části implementace. Všechny části, tedy server, šifrovací knihovna i aplikace pro vyhledávání byly plně funkční.

Diplomant pohotově reagoval na mé otázky a celkově projevil odpovídající znalost dané problematiky. Nahlédli jsme i do zdrojových kódů, implementace byla správně rozčleněna do jednotlivých komponent a z mého pohledu velmi přehledná. Celkově implementaci hodnotím pozitivně.

Otázky

- Jak nejlépe integrovat implementovanou knihovnu s již existujícím systémem, kde auditní logy vznikají?

- V rámci testů byl proveden také benchmark hashovacích funkcí. Bylo by možné obdobným způsobem provést zátěžový test celého systému? Jak by se při takovém testu postupovalo?

Závěr

Celkově považuji diplomovou práci za zdařilou. Autor splnil zadání ve všech jeho bodech. Vzhledem ke všem výše zmíněným nedostatkům textu hodnotím známkou ***C – dobře***.

V Praze dne 18. 6. 2020 Ing. Jan Smejkal