Posudek vedoucího diplomové práce

Zadané téma: Vyhledávání nad šifrovanými daty v aplikacích s architekturou klient-server
Student: Bc. Lukáš Toman
Vedoucí práce: Ing. Martin Mudra
Oponent Práce: Ing. Jan Smejkal

Téma práce

Téma práce se zabývá implementací proof-of-concept systému, který umí data zašifrovat, přenést na sever a následně nad nimi dělat vyhledávací operace bez nutnosti znalosti dešifrovacího klíče. Aplikace této metody byla v rámci zadání již omezena na data z auditních logů externích systémů.

Průběh práce

Velkou částí práce pana Tomana byla analýza existujících řešení a zhodnocení jejich použitelnosti. Poskytnuté materiály byly převážně vědecké články popisující několik metod. S panem Tomanem jsme měli několik schůzek, kdy zejména v počátku byl vidět velký zájem o téma a chodil vždy připraven. V druhé části, zejména s blížícím se koncem se však průběžná práce zhoršila. Pan Toman, zejména v průběhu analytické fáze, chodil s množstvím nových materiálů a vzhledem k tomu, že se jednalo o téma spíše výzkumné hodnotím tento fakt velmi kladně. Pozitivně se také podepsal kurz kryptografie, který pan Toman dobrovolně absolvoval v online režimu na jiné univerzitě. Zejména analytické části se zhostil samostatně a zodpovědně. Bohužel do psaní textové části práce bylo nezbytné pana Tomana mírně pobízet k jejímu dokončení.

Text práce

Struktura hlavních kapitol textu práce splňuje obvyklé a logické konvence technického textu. Směřování tématu práce vedlo na několik metod a bylo nezbytné důsledně analyzovat vhodnost těchto algoritmů pro téma auditního logování. Bohužel samotný popis algoritmů je napsán poměrně a text je rozdělen převážně do velmi krátkých podkapitol, což velmi zhoršuje samotnou čitelnost. Některé kapitoly jsou složeny převážně z bodových seznamů a působí tak krátce, neukončeně a uměle práci pouze natahují. Práce je doplněna obrázky, na které však není z textu velmi často odkaz. Bez příslušné znalosti tématu a problematiky je problém pochopit jejich význam a umístění. Textová část práce, zejména část Analýza, by mohla čerpat z většího množství literatury. Obzvláště kapitoly v části návrhu předkládají tvrzení, která nejsou plně zacitována a doložena ať již citací příslušného zdroje nebo odkazem na kapitolu, která toto tvrzení dokazuje. Samotné citace jsou také velmi často až za větou. Konec kapitoly testování je vyloženě odbytý a je na ní vidět, že autorovi již docházely síly a čas. Proti navržené metodice testování však větších výhrad nemám.

Použitou literaturou jsou převážně články popisující samotné algoritmy a webové zdroje, což je vzhledem k tématu pochopitelné. Zejména přehlednost textu a práce se zdroji nejsou silnou stránkou textové části a celkově bych ji hodnotil spíše známkou **D – Dostatečně**.

Implementace a Testování

Implementované řešení je plně funkční, obsahuje veškerou potřebnou funkcionalitu a je vhodně rozděleno do jednotlivých knihoven. Zdrojový kód je poměrně přehledný, i když obsahuje prvky, které nejsou vždy úplně dotažené. Samotné algoritmy byly nakonec implementovány poměrně krátkým kódem, což je za vděk především vhodnému výběru platformy. Kód bohužel neobsahuje žádný komentář. Alespoň hlavní třídy bych si představoval okomentované formou komentářové dokumentace. I přes tento nedostatek jsem však neměl výraznější problém kód pochopit. Samotné implementační části lze vytknout nedostatek dokumentace a odbyté testování a ohodnotil bych ji známkou **B – Velmi dobře**.

Závěr

Téma práce bylo zaměřené převážně na výzkum metod z vědeckých článků a jejich následné převedení do aplikace nad strukturovaným textem. Student se dokázal v problematice zorientovat, analyzovat metody a samostatně vyvinout a popsat jeho dílo. Samotný průběh práce se postupem času zhoršoval a odkládal, což se bohužel negativně podepsalo na kvalitě textové části práce. Výsledné hodnocení vzhledem k výše uvedeným faktům a s přihlédnutím k samotnému průběhu tak hodnotím známkou **C – Dobře.**

V Praze dne 16. 6. 2020

Ing. Martin Mudra

Ing. Martin Mudra
Digitally signed by Ing. Martin Mudra
Date: 2020.06.17 00:35:38 +02'00'