Posudek oponenta bakalářské práce

Student: Sadloň Matej
Téma: Databázové úložiště virtuální čekárny (id 17659)
Oponent: Brejcha Jan, Ing., UPGM FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

2. Splnění požadavků zadání **zadání splněno pouze částečně**

Dle mého názoru si autor velmi usnadnil práci a předvedl řešení, které je příliž jednoduché a rozsahu bakalářské práce odpovídá pouze stěží. Řešení je navíc nedostatečné i v rámci tématu virtuální čekárny. Autor navrhuje použití databáze MySQL coby databázového serveru. Zcela zde chybí rešerše databázových enginů a analýza, která by ukázala správnost volby MySQL. Je provedena pouze krátká rešerše dvou existujících "vyvolávacích systémů" bez speciálního zaměření na databázi. Bod 1 zadání je tedy splněn pouze z části. Autor navrhuje velmi jednoduché schéma databáze, které postrádá důležité části pro implementaci zamýšlené funkcionality, jak autor sám přiznává v závěru práce. Požadovaná koncepce z bodu 2 zadání tedy vytvořena byla, ale pouze ve ve velmi omezeném rozsahu. Bod 3 nebyl dle mého názoru v práci řešen vůbec - autor se diskusí vlastností navržené koncepce a dopady na výkon a velikost dat vůbec nezaobíral. To je dle mého názoru velká chyba, protože navrhované řešení bude mít velké problémy se škálovatelností i bezpečností, což jsou klíčové požadavky na databázi tohoto typu. Bod 3 tedy nebyl dle mého názoru splněn vůbec. Bod 4 požaduje implementaci databázového úložiště a demonstraci implementace na vhodném příkladě. Autor sice vytvořil implementaci navrhovaného konceptu databáze s knihovnou pro snažší volání předem definovaných funkcí, avšak testovací aplikace testuje pouze vytvoření struktury tabulek - podnik, fronty, služby, ale již např. neumožňuje zápis klienta do fronty, či jeho vyřazení. Stěžejní funkce - zápis uživatele do fronty - není tedy demonstrována vůbec.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

Text technické zprávy je v obvyklém rozmezí. Problém spatřuji v tom, že velkou část (cca 10 stran) zabírá dokumentace funkcí implementovaných v knihovně komunikující s databází, přičemž tuto dokumentaci není nutné uvádět do technické zprávy. Vzhledem k tomu, že se jedná pouze o seznam metod a jejich argumentů, které jsou popsány pouze stroze, doporučil bych takovou dokumentaci vygenerovat a přiložit zvlášť, jako přílohu (např. pomocí nástroje Doxygen).

4. Prezentační úroveň předložené práce **65 b. (D)**

Text technické zprávy je členěn srozumitelně a logicky. Zde bych vytknul použití nadpisu třetí úrovně v sekci 5.2, kde jsou popsány jednotlivé funkce knihovny. Důvodem je příliž jemné dělení - na jedné stránce jsou tak i 4 nadpisy, což je nevhodné. Celková struktura dokumentu je logická, kapitoly na sebe navazují. Dále chci upozornit na fakt, že rozsah kapitoly 6 Testování pokrývá pouze čtvrtinu stránky a žádné testování ani jeho výsledky zde popsány nejsou.

5. Formální úprava technické zprávy **75 b. (C)**

Formální úprava technické zprávy je průměrná. Vyskytují se poměrně velké obrázky, které by bylo možno zmenšit, obrázky jsou však kvalitní a dobře čitelné. Jazyková stránka práce se mi nehodnotí snadno, jelikož se jedná o slovenský text, nicméně na žádné překlepy jsem nenarazil. Častěji se však vyskytují typografické chyby, zejména spojky a předložky na konci řádků, nebo např. absence mezery před citací.

6. Práce s literaturou **50 b. (E)**

Seznam literatury obsahuje celkem 11 referencí, z toho 6 z nich je na Wikipedii, což mi přijde silně nevhodné. Vzhledem k tomu, že se jedná o reference na technologie typu PHP, Apache, MySQL, apod., jistě se nechají dohledat relevantnější publikace, např. ve formě knih, či alespoň webová dokumentace přímo ze zdroje. Vůbec jsem nepochopil odkaz na referenci [1], který se nachází na straně 16 na konci prvního odstavce sekce 4.4., dle mého názoru je zde citace zvolena nevhodně.

7. Realizační výstup **50 b. (E)**

Realizační výstup je velmi slabý. Sestává se z návrhu databázového schématu, knihovny pro komunikaci s databází a testovacího klienta. Knihovna pro komunikaci s databází je vytvořena velmi jednoduše, víceméně pouze zapouzdřuje volání SQL dotazů do databáze s určitými argumenty. Problémem je, že knihovna se nezabývá escapováním vstupních argumentů, používá pouze metodu strip_tags na odstranění HTML tagů. Útočník tedy bude schopen provést útok pomocí SQL Injection. Rozumnější by bylo využít pro tuto část nějaké ORM vrstvy (např. Symphony, apod.), která od psaní SQL příkazů abstrahuje, navíc tím, že je generována ze schematu databáze je snadno upravitelná v případě, že se databázové schema změní. Navíc implementace php

knihovny je dle mého názoru nedostatečná. V případě, že by další části tohoto distribuovaného systému byly napsány v jiném programovacím jazyce (např. Java), je tato knihovna nepoužitelná. Jako rozumnější řešení by mi přišlo oddělit databázovou část do samostatné webové aplikace, která by umožňovala pomocí nějakého protokolu komunikaci s databází. Implementovaný klient je taktéž značně jednoduchý a neobsahuje všechny funkce nutné pro otestování funkčnosti databáze alespoň pro základní použití (např. zapsání zákazníka do fronty). Zde také musím upozornit na fakt, že po instalaci klienta na server a po instalaci databáze bylo nutno opravit chybu na řádku 174 v souboru Lib.php - v tabulce vytvořené dodaným schematem chybí sloupec 'Created' a aplikace tedy hlásí chybu Column 'Created' not found.

8. Využitelnost výsledků

Vhledem k tomu, že se autor nezabýval možností škálování databáze do budoucna, bezpečností, ani rigorózním návrhem, jsou výsledky této práce velmi těžko použitelné pro další vývoj systému.

9. Otázky k obhajobě

- Jakým způsobem byste řešil škálování stávajícího řešení na více strojů?
- Jakým způsobem byste zpřístupnil Vaše API v případě, že databáze poběží na jiném serveru, než hlavní aplikace? Berte v úvahu, že hlavní aplikace může být napsána i v jiném jazyce, než je napsána Vaše část.

10. Souhrnné hodnocení **50 b. dostatečně (E)**

Celkové hodnocení nejvíce ovlivnil fakt, že navrhované řešení je dle mého názoru nedostačující potřebám distribuovaného systému "Virtuální čekárna". Naprosto chybí rešerše databázových enginů. Z tohoto důvodu student následuje volbu MySQL, místo toho, aby zvolil vhodnější databázi vhodnou pro distribuované systémy a velká data. Kapitola 6 Testování má pouze čtvrt stránky ve dvou odstavcích a nejsou zde uvedeny žádné výsledky. Implementace databázové knihovny obsahuje zásadní bezpečnostní díry (např. není řešeno escapování a kód je náchylný k útokům typu SQL Injection). Navíc implementace testovacího klienta neobsahuje všechny funkce potřebné pro verifikaci, zda je databázové úložiště navrženo správně. Ve výsledném hodnocení přihlížím k faktu, že ač je výsledná aplikace velmi jednoduchá, je až na detail zmíněný výše funkční.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 2. června 2016

.....
podpis