Oponentský posudek disertační práce

Autor: Ing. Radek Šilhavý

Téma: Experimentální ověření distribuovaného volebního schématu

Volby jsou jedním z klíčových komponent demokratického procesu, tradiční volby jsou založené na fyzické účasti voliče ve volební místnosti a manuální papírové manipulaci s hlasy (včetně počítání hlasů). Využití on-line technologií pro volební systém je potom dalším logickým krokem, který bude následovat.

Předložená disertační práce se zabývá důležitou a současně teoreticky velmi náročnou problematikou. V práci jsou představeny možné přístupy k elektronickým volbám bez nutnosti fyzické účasti ve volební místnosti. Byla navržena metodika elektronických voleb pod názvem distribuované volební schéma. Navržené schéma bylo experimentálně testováno na simulovaných volbách do senátu Fakulty aplikované informatiky.

Aktuálnost disertační práce

Je zřejmé, že zpracované téma je vysoce aktuální, nejen po technické stránce řešení problému, a zaslouží si pozornost odborné veřejnosti. Právní záležitosti ohledně možnosti elektronického hlasování musí být explicitně ošetřena v zákoně (popřípadě v předpisech organizace – univerzity). Ve světě již probíhají pilotní projekty, které se snaží odbourat papírové medium a nahradit ho elektronickým hlasovacím zařízením. V ČR se problematikou elektronických voleb zabývá od roku 2006 komise ministerstva vnitra spolu s Českým statistickým úřadem. Výsledky práce této komise nebyly dosud zveřejněny.

Vědecký přínos práce

Přínos práce spočívá jak v teoretické, tak aplikační oblasti. Práce má dobrou úroveň. Za původní teoretický přínos lze označit navržené distribuované volební schéma, které vzniklo vhodnou kombinací známých a již využívaných metod.

Publikační aktivity

Disertant ve své publikační činnosti uvádí více než dvacet příspěvků, z nichž asi polovina se přímo týká zpracovaného tématu. Dílčí výsledky tedy byly diskutovány s širokou odbornou veřejností.

Další vyjádření k práci

Na straně 28, v bodě 10 (také na straně 30, bod 6) je uvedeno: „Pokud volič hlasoval ve volební místnosti, nebude možné již hlasování elektronické." Přitom v textu (předchozí bod) se počítá s anulováním elektronických hlasů až po uzavření volebních místností. Záleží tedy pouze na technickém řešení, které může umožnit pozdější elektronické hlasování (i když nebude započítáno).

Na straně 30 se v kapitole 3.8 odkazuje na obrázek 7, kde je zobrazena autorizace pomocí LDAP, což není v textu popsáno. Předpokládám, že si je disertant vědom toho, že v publikovaných experimentálních volbách v síti UTB dochází k přenosu hesla v nešifrované podobě. V kombinaci s navrženým vícenásobným hlasováním je zde slabé místo, přes které by šlo zmanipulovat volby.

Kapitola 4.2.2.3 na straně 43 je podmnožinou předchozí kapitoly (viz. Případ užití Zobrazení hlasovacího lístku, bod 3.1 na straně 42. Kapitola je tedy dle mého názoru zbytečná.

Obrázek 16 na straně 49 prezentuje v diagramu po validaci dat chybovou hlášku a posléze pokračování běhu aplikace. Tato akce není v textu diskutována. Dle mého názoru by měl být volič vyzván k úpravě dat tak, aby byly validní. Pokud tedy volič nechce cíleně odevzdat neplatný hlas.

Strana 50, obrázek 17. Rozdělení na tři aktéry je nešťastné, protože za celkový průběh voleb zodpovídá volební komise. Administrátor a jeho případy užití by tedy měly spadat pod zodpovědný orgán. Akce „Zavedení volebních lístků" u administrátora voleb má uvedeno, že ji provádí volební komise, což neodpovídá navržené struktuře. V obrázku 17 „Případy užití pro jednotlivé aktéry v části B" jsou uvedeny dva případy užití, které v této části textu nejsou popsány a patří do části C.

Strana 54, v textu je uvedeno „začíná přihlášením uživatele", správně má být „začíná přihlášením administrátora".

Strana 55, na obrázku 19 je uvedeno „Administrátor volí zadávání volebních okrsků“, správně má být „Administrátor volí zadávání kandidátních listin“. Nelogické je i provedení výběru volebního okrsku a až poté zobrazení seznamu volebních okrsků. Obrázek tedy neodpovídá případu užití „Zavedení kandidátních listin“ (ID 7), který se na něj odkazuje.

Strana 66, kapitola 4.3.1.7 Prezence voliče. Obecně bych doporučoval dodatečný kontrolní mechanismus při presenci voliče – např. zadáním čísla OP nebo RČ. Zamezí se tím možnosti, kdy komise může cíleně anulovat elektronické hlasy tím, že fiktivně zaregistruje voliče ve volební místnosti.

U realizace experimentu postrádám zveřejnění WWW adresy, aby oponent, případně komise měla přístup do popisované aplikace. V práci také dále postrádám popis struktury databáze.

Stěžejní u tohoto typu aplikace by mělo být zabezpečení. Tato pasáž je dle mého názoru popsána nedostatečně. V textu práce je zmíněno šifrování veřejným klíčem komise, není ale zmíněno, jaký algoritmus je využíván. V textu také chybí popis dat, která se veřejným klíčem šifrují. V případě že se jedná pouze o identifikační číslo kandidáta z databáze, tak při výběru stejného kandidáta a použití stejného veřejného klíče dostaneme stejný výsledek a půjde velmi jednoduše poznat, kteří voliči hlasovali stejně. Tento krok (šifrování veřejným klíčem) by potom byl zbytečný, doporučuji proto zahrnout do šifrovaných údajů nějaký jedinečný údaj, např. časovou známku. Nedostatečně popsáno je i následné aplikování elektronického podpisu. Elektronický podpis přece obecně složí jako ochrana proti modifikaci údajů, ale zároveň jednoznačně identifikuje svého majitele. Obsah této kapitoly jde charakterizovat slovy: „Více otázek jak odpovědí“.

Při experimentálním ověřením bylo předpokládáno, že student FAI náleží do kontextu fai-st, což bohužel není pravda. Jediný možný zdroj všech oprávněných voličů je studijní systém STAG. Systém také nebere v úvahu výběr volebního okrsku v případě studentů doktorandů – zaměstnanců.

Strana 79, v textu je dvakrát chybně uveden dotaz do ankety na téma vyšší volební účast.

V textu disertační práce není uveden počet studentů, kteří se zúčastnili ankety. Výsledné grafy neberou ohled na počty studentů a jsou interpretovány chybně.

- Obrázek 32 je interpretován jako: „největší zájem měl druhý ročník". Přesto podle absolutního počtu studentů v ročníku a procentuálního zastoupení ve volbách si troufám tvrdit, že největší zájem měli studenti pátého ročníku.
- Procentuální účast žen je prezentována jako slabá, ale dle mého názoru poměr přibližně odpovídá procentuálnímu zastoupení studentek na fakultě aplikované informatiky.
- Z grafu na obrázku 35 nelze vyčíst vyšší volební účast v porovnání s reálnými volbami. Graf pouze říká, že z celkového počtu účastníků se 25% zúčastnilo reálných voleb do AS FAI.
- Rozdíly výsledků průzkumu v otázkách celkové hodnocení, ovladatelnost a doporučení kolegům odpovídají spíše statistické odchylce a nelze z nich dělat konečné závěry.

Strana 82, na pravou míru je potřeba upřesnit studijní program Inženýrská informatika a studijní obory Informační a řídicí technologie a Bezpečnostní technologie, systémy a management.

Strana 87, v textu je uvedeno, že ovladatelnost systému kladně hodnotí více než 90% uživatelů, ale v grafu je prezentováno 95%.

Připomínky k formální úrovni práce

V celé práci disertant zásadně používá nelogické slovní obraty typu „na obrázku Obrázek X".

Tabulky případů užití nejsou řádně popsány a číslovány.

Strana 26, odst. 1: místo „ … téměř s jistou …" má být „ … téměř s jistotou …".

Strana 42, scénář: slovo Include.

Strana 42, odst. 2: místo „… kandidátní listin" má být „… kandidátních listin".

Strana 43, odst. 2: místo „Případů užití" má být „Případ užití".

Strana 66, scénář: slovní spojení: „... zvolí vybere voliče".

Strana 66, odst. 1: místo prezentace má být prezence.

Strana 73, odst. 2: Je uvedeno, že nebyla použita jména reálných osob, avšak obrázek 29 na straně 76 zobrazuje jména skutečných kandidátů.

Strana 74, odst. 1: místo „... technologu skriptování ...“ má být „... technologie skriptování ...“

Strana 92, odst 1: místo „Výhodu ...“ má být „Ve výhodu ...“.

Strana 97,odst 2: místo „... volebního procesů“ má být „... volebních procesů“.

Strana 99, nadpis: místo „Směry dalšího výzkum“ má být „Směry dalšího výzkumu“.

Strana 99, odst. 2: chybějící čárka „...experimentu, respektive ...“.

Strana 100, odst. 5: místo „... zejména potřeba ...“ má být „ ... zejména potřebám ...“.

Strana 107: příliš časté střídání slov prezenční a presenční.

Otázky na disertanta

1. Při obhajobě disertační práce žádám disertanta, aby se k výše uvedeným výtkám ohledně bezpečnosti v rámci diskuze vyjádřil.
2. Jakým způsobem budete reagovat na fakt, že grafické ztvárnění nevyhovuje 20% uživatelů? V případě WWW prezentace komerční firmy by se jednalo o neakceptovatelné číslo. Jak budete reagovat na fakt, že 10% vysokoškoláků neporozumělo instrukcím?
3. V životopise uvádíte přípravu pěti žádostí o grantové projekty. Kolika projektů se aktivně účastníte, nebo jste se zúčastnil?

Závěr

Disertační práce Ing. Radka Šilhavého je zpracována na dobré odborné úrovni. Přináší nové poznatky, ukazuje na jeho odborné schopnosti, znalost řešené problematiky i na jeho způsobilost k samostatné tvůrčí vědecké práci.

Práci doporučuji předložit k obhajobě.

Ve Zlíně dne 27. 11. 2009 .....

doc. Ing. Martin Sysel, Ph.D.

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Nad Stráněmi 4511
760 05 Zlín

Vysoké učení technické v Brně
Fakulta podnikatelská
Ústav informatiky
prof. Ing. Jiří Dvořák, DrSc.

Oponentský posudek disertační práce

Autor práce: **Ing. Radek ŠILHAVÝ**

Název práce: **EXPERIMENTÁLNÍ OVĚŘENÍ DISTRIBUOVANÉHO VOLEBNÍHO SCHÉMATU**

V předložené disertační práci jsou řešeny aktuální přístupy k elektronickým volbám. Autor klade důraz na model internetového volebního systému. Práce vychází ze systémového pojetí distribuovaného volebního schématu a z výzkumů elektronického prostředí veřejné správy.

V předložené práci se autor také opírá o historické změny systémů hlasování z pohledu technických možností, technologických a komunikačních elektronických prostředí a sociálních aspektů ve vývoji volebních systémů. Autor se v dalším správně zabývá možnostmi současných informačních a komunikačních technologií a zejména se soustřeďuje na možnosti Internetu.

Cílem výzkumu bylo modelově zachytit systém organizace vzdáleného hlasování, který by umožnil plnit volební proces v demokratické společnosti. V souladu s tím výzkum řešil možnosti základní podmínky volebního systému v moderních prostředích elektronické komunikace a to s uvažováním ověření voliče a jeho tajného přístupu k volbě např. opakovanou volbou při jednoznačném tajném vyjádření ke kandidátům volebního aktu. Významnou oblastí výzkumu byla také ochrana osobních dat a s tím i spojená bezpečnost odpovídajících bází dat.

Autor správně věnoval pozornost zhodnocení současného stavu řešené problematiky (kap.2–Teoretický rámec) a popisu vybraných problémů v publikovaných materiálech vztahujících se k řešené problematice. Zajímavé jsou dílčí zkušenost uvedené v kap.2.7.

Experimentální část, uvedená v kapitole třetí, je výchozím sdělením o cíli práce (kap. 3.2) – autor zde vychází ze systémově pojatého volebního procesu dovedeného do konceptuálního modelu návrhu řešení distribuovaného volebního systému a ověření prototypu webového volebního schématu s identifikací klíčových míst pro budoucí modelování volebního systému. Autor správně reaguje na podmínky možného bezpečného modelu (kap.3.9.).

Významné místo v práci má konceptuální návrh řešení (kap.4.). Správně hierarchicky uspořádává základní vlastnosti systému a vypracovává v části A odpovídající scénáře. Grafické vyjádření odpovídajících diagramů v dalších částech práce považuji za zdařilé a za způsob velmi dobrého sdělování informaci o daném problému.

Realizace experimentu a odpovídajícího rozboru výsledků experimentování, uvedená v kapitolách páté a šesté, jsou přiblížením možných modelových představ na zjednodušeném prostředí voleb AS.

Využitelnost modelu uvedená v sedmé kapitole je stručným vymezením modelu řešeného problému. Zobecňující prostředí je velmi obtížné identifikovat s ohledem na specifické prostředí elektronického hlasování v obecném časoprostorovém vyjádření.

Autor velmi dobře vyjádřil vybraný pojmový aparát a vymezil model současného stavu zkoumání specifického sociálně technického modelu a legislativních rámců v modelování a elektronizaci volebního procesu.

Podařilo se mu charakterizovat prostředí možného vytváření modelu volebního procesu, ověřit jeho dílčí specifické chování, nastínit řadu otázek spojených s bezpečnosti a riziky těchto rozsáhlých modelů v elektronickém prostředí a upřesnit další možné cesty výzkumu v této zajímavé a perspektivní cestě elektronického obchodu s informacemi.

Pozitivně hodnotím na předložené práci to, že autor vyjádřil vhodně verbální modelování. Správně definoval rozlišovací úroveň systému a ukázal možnou identifikovatelnost uvedených procesů.

Po stránce formální je celá práce zpracována svědomitě s odpovídající úrovní sdělování. Předložená práce svědčí o cílevědomém přístupu autora k řešené problematice, předpokladech autora k formulování této aktuální problematiky.

V diskuzi by se měl vyjádřit autor k následujícím otázkám:

1. Jak se do modelu promítnou další možné podsystémy – například monitorování nebo důvěryhodnosti voleb?
2. Stručně vyjádřete vědecký přínos práce pro rozvoj vědního oboru.

V práci se vyskytují některé drobné nedostatky: např. u grafů, obrázků a diagramů chybí uvedení zdrojů (resp. zápis např. „vlastní"), str. 3 a 7 jsou volné listy, uvedení obrázek č. a za tím nadpis graf je dost neobvyklé, použitá literatura není setříděna podle abecedy apod. V uvedeném modelu postrádám matematické vyjádření alespoň dílčích problémů tak, aby byl vytvořen základ pro budoucí modelování na modelu volebního systému.

Autor předložené práce splnil uvedené cíle a na modelu ověřil aplikace elektronického volebního systému založeného na vzdáleném hlasování.

Na základě všech zmíněných skutečností konstatuji, že autor prokázal schopnost a připravenost k samostatné tvůrčí činnosti.

Disertační práci doporučuji k přijetí a po úspěšném obhájení práce udělit Ing. Radku Šilhavému titul Ph.D.

V Brně dne 1. listopadu 2009

prof. Ing. Jiří Dvořák, DrSc..

Oponentní posudek doktorské disertační práce

Jméno oponenta: doc. Dr. Ing. Oldřich Kodym

Jméno disertanta: Ing. Radek Šilhavý

Název práce: Experimentální ověření distribuovaného volebního schématu

---

A. Aktuálnost zvoleného tématu

Orgány řídící demokratickou společnost jsou ustanovovány dle vůle občanů. Tato vůle je ve stanovených časových intervalech zjišťována volbami. V posledních letech lze pozorovat trend snižování ochoty občanů tuto vůli projevit. Tento jev má více příčin, které však jsou mimo základní zaměření práce. Práce disertanta se zaměřuje na vlastní volební akt s využitím aktuálních prostředků informačních a komunikačních technologií (ICT). Je to jedna z cest, jak volební akt zjednodušit a přiblížit občanům a tím zvýšit podíl těch, kteří volbou složení zastupitelských orgánů ovlivňují.

Závěr bodu A

Téma disertační práce považuji za vysoce aktuální.

B. Cíle práce

(*zhodnocení vytýčených cílů práce a zhodnocení, jak disertant stanovené cíle splnil*)

Disertant si v předložené práci stanovil 4 cíle: studium aktuálního stavu, návrh řešení, realizace experimentu a zpětná vazba spolu s návrhem dalšího postupu. Tyto cíle na sebe logicky navazují. Důraz je v práci kladen především na 3. Cíl – praktický experiment. Všechny cíle jsou v práci přehledně zpracovány.

Závěr bodu B

Dílčí cíle naplňují hlavní cíl disertační práce. Disertant jak dílčí tak i hlavní cíl disertační práce splnil.

C. Zvolené metody zpracování a postup řešení

(vyjádření ke zvoleným metodám a k postupu řešení problému)

V práci autor použil analytické i empirické metody a postupy jak v oblasti hodnocení aktuálního stavu v zájmové oblasti tak i při vlastním návrhu a hodnocení

Disertační práci považuji za významnou jak pro obor disertanta tak i pro mnohé společenskovědní obory.

Publikační aktivita disertanta

(vyjádření k publikační aktivitě diletanta)

Autor v předložené práci uvádí celkem 21 publikací z období 2004-2008, z toho 3 kde je jediným a 10 kde je prvním autorem. 9 publikací je tématiky svázáno s předloženou prací.

Závěr bodu F

Publikační aktivity autora jsou přiměřené s výhradou nulové aktivity v tomto roce.

Formální úprava disertační práce a jazyková úroveň

(Vyjádření ke struktuře disertační práce, k formálnímu zpracování a k jazykové úrovni)

Práce je zpracována přehledně, jednotlivé kapitoly na sebe logicky navazují. Autor zařadil obrázky přímo do textu, což přispívá k orientaci čtenáře v předložené problematice. Jazyková úroveň práce je vysoká, několik pravopisných chyb/překlepů ji nikterak nesnižuje.

Některé použité formulace především v úvodní části však nejsou přesné. Např. na straně 9 „...musí volit pouze jednou..." zakládá volební povinnost nikoliv právo; opomenutí samosprávy v 1. odstavci kapitoly 2.6. Teprve v podkapitole Skupování hlasů (str. 95) je uvedeno, že u elektronické volby platí poslední hlas. Jinde v práci, kde by tato informace měla být uvedena, zvolil autor bohužel formulaci velmi neurčitou.

Závěr bodu G

Formální i jazyková úroveň práce je velmi dobrá.

Připomínky k disertační práci

(konkrétní připomínky k disertační práci)

Kdo vytvořil volební systém použitý v experimentu?

Jakým způsobem je realizováno losování při rovném počtu hlasů více kandidátů?

Jak je nebo jak by mohlo být zajištěno, aby volbu neprovedla za oprávněného voliče třetí osoba?

Co je to autentizace a jak je zabráněno zneužití autentizačních prvků (PIN...) na straně voliče?

Závěrečné zhodnocení

(celkové zhodnocení disertační práce a jednoznačné vyjádření, zda oponent práci ***doporučuje*** *nebo* ***nedoporučuje*** *k obhajobě)*

Předložená práce mne velmi zaujala jednak řešeným tématem a i svým zpracováním. Jak už jsem uvedl dříve práce řeší významnou celospolečenskou problematiku využitím informačních a komunikačních technologií.

Z dílčích hodnocení v předchozích bodech vyplývá, že práce i ostatní aktivity disertanta odpovídají požadavkům pro absolvování doktorského stupně studia, proto ji **doporučuji k obhajobě**.

V Ostravě 27. listopadu 2009

.....

podpis oponenta