UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Gabriel Garcia Becker

Lucas Pandolfo Perin

INTEGRIDADE DE BANCO DE DADOS

Florianópolis(SC)

2012

UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Gabriel Garcia Becker

Lucas Pandolfo Perin

INTEGRIDADE DE BANCO DE DADOS

Trabalho de Conclusão de Curso

Ciências da Computação

Orientador: Marcelo Carlomagno Carlos

Professor Responsável: Ricardo Felipe Custódio

UFSC

Florianópolis(SC)

2012

FOLHA DE APROVAÇÃO DE PROPOSTA DE TCC

Acadêmico	Gabriel Garcia Becker Lucas Pandolfo Perin
Título do trabalho	Integridade de Banco de Dados
Curso	Ciência da Computação/INE/UFSC
Área de Concentração	Ciências Exatas e da Terra/Ciência da Computação/Metodologia e Técnicas da Computação/Segurança em Computação

Instruções para preenchimento pelo ORIENTADOR DO TRABALHO
- Para cada critério avaliado, assinale um X na coluna SIM apenas se considerado aprovado. Caso contrário, indique as alterações necessárias na coluna Observação.

Critérios	**Aprovado**				**Observação**
	Sim	**Parcial**	**Não**	**Não se aplica**	
1. O trabalho é adequado para um TCC no CCO (relevância / abrangência)?					
2. O titulo do trabalho é adequado?					
3. O tema de pesquisa está claramente descrito?					
4. O problema/hipóteses de pesquisa do trabalho está claramente identificado?					
5. A relevância da pesquisa é justificada?					
6. Os objetivos descrevem completa e claramente o que se pretende alcançar neste trabalho?					
7. É definido o método a ser adotado no trabalho? O método condiz com os objetivos e é adequado para um TCC?					

8. Foi definido um cronograma coerente com o método definido (indicando todas as atividades) e com as datas das entregas (p.ex. Projeto I, II, Defesa)?					
9. Foram identificados custos relativos à execução deste trabalho (se houver)? Haverá financiamento para estes custos?					
10. Foram identificados todos os envolvidos neste trabalho?					
11. As formas de comunicação foram definidas (ex: horários para orientação)?					
12. Riscos potenciais que podem causar desvios do plano foram identificados?					
13. Caso o TCC envolva a produção de um software ou outro tipo de produto e seja desenvolvido também como uma atividade realizada numa empresa ou laboratório, consta da proposta uma declaração (Anexo 3) de ciência e concordância com a entrega do código fonte e/ou documentação produzidos?					

Avaliação	☐Aprovado	☐Não Aprovado
Ricardo Felipe Custódio	03/07/2012	
Marcelo Carlomagno Carlos	03/07/2012	

RESUMO

A verificação da integridade de um banco de dados pode não ser tão fácil como consultar os logs de um SGBD. Deve-se prover ferramentas para garantir a privacidade, integridade e confiabilidade das informações contidas em um banco de dados. Este trabalho visa desenvolver uma biblioteca para a solução desde problema e um protótipo para prova de conceito.

Palavras-chave: Segurança em Computação, Banco de Dados, Integridade, Privacidade, Confiabilidade, Criptográfia

SUMÁRIO

Introdução

Através do crescente uso de computadores e da internet podemos dizer que temos , hoje, acesso quase ilimitado à informação. Mesmo quando pensamos em informações secretas e protegidas por empresas, por exemplo, é difícil se imaginar um sistema completamente seguro de *hackers*. Informações, estas, que são armazenadas em todo o mundo. Acessamos informações guardadas em outros computadores ou servidores o tempo todo enquanto navegamos na internet. Muito frequentemente são utilizados bancos de dados dos quais estão instalados em grandes *Data centers* que disponibilizam seu conteúdo para uso na *Web*.

Quando se trabalha com dados pessoais, empresariais ou qualquer tipo de dado que deve ser mantido confidencial, é necessário fazer uso de métodos que garantam a integridade e sigilo destes. Bancos de dados são ferramentas muito poderosas para armazenar e organizar qualquer tipo de dado mas mesmo estes não garantem sigilo total e integridade dos dados neles armazenados.

É proposto, neste trabalho, uma solução para sigilo de dados e integridade de um banco de dados. Serão usados também algoritmos criptográficos para a cifragem dos dados (garantindo assim o seu sigilo), verificação e validação.

Lista de abreviaturas e siglas

PKCS – Public Key Cryptography Standards

HSM – Hardware Security Module

TPM - Trusted Platform Module

1. Objetivos

Este trabalho, tem como objetivo criar uma biblioteca JAVA com interfaces que ofereçam suporte a operações de verificação de integridade e privacidade de um banco de dados. A biblioteca deverá conter suporte a dispositivos criptográficos como PKCS#12, HSM, TPM, SmartCard e Token.

Devera ser feito também, um protótipo, com um pequeno banco de dados, para prova de uso da biblioteca implementada.

2. Métodos de Pesquisa

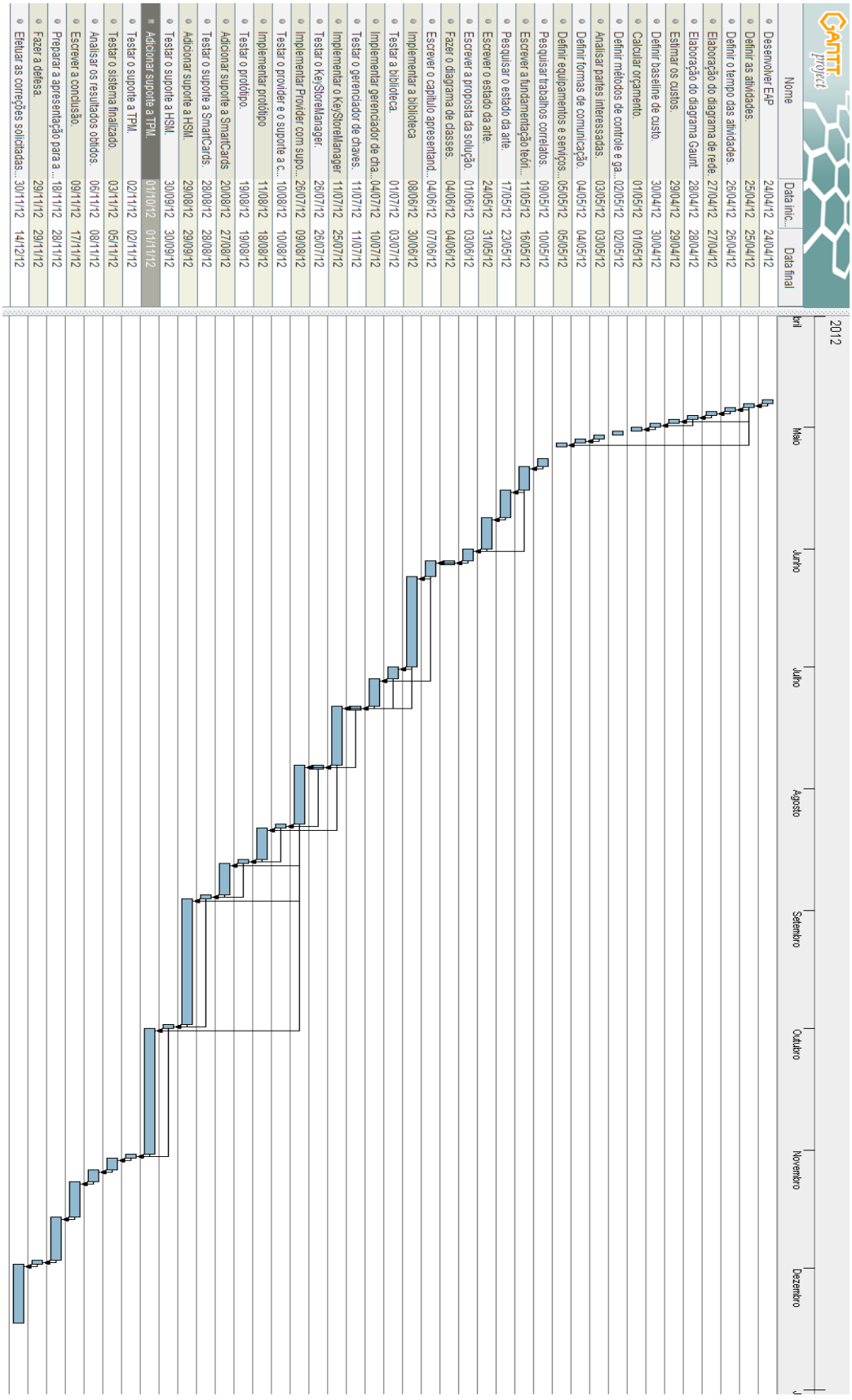
O trabalho será desenvolvido em etapas, tais etapas têm seu cronograma restrito pelas datas limites impostas pelas disciplinas Introdução ao TCC, Trabalho de Conclusão de Curso I e II, portanto o trabalho será executado de forma a atender esse cronograma imposto. O trabalho sera divido em diversas etapas, pesquisa, desenvolvimento da biblioteca, suporte a diversos dispositivos criptográficos e desenvolvimento de um protótipo.

A primeira etapa consiste em pesquisar as soluções necessárias para satisfazer os pré requisitos do projeto, que são, garantir a integridade, autenticidade, confiabilidade e privacidade de um banco de dados.

A segunda etapa consiste em implementar uma biblioteca que proverá as funções para garantir os objetivos do projeto. Nas seguintes etapas, iremos adicionar suporte a diversos dispositivos criptográficos, PKCS#12, SmartCars, HSM e TPM.

Na ultima etapa será desenvolvido um protótipo, com um pequeno banco de dados, para prova e demonstração das funções implementadas na biblioteca, testes de desempenho serão feitos nesta etapa.

3. Cronograma



4. Custos

Item	Quantidade	Valor unitário	Valor total
PESSOAL			
Pesquisador	2(11 meses – 4h/dia)	R$25,00	R$11.000,00
Programador	2(7 meses – 6h/dia)	R$25,00	R$7.000,00
Banca	1	R$840,00	R$840,00
Orientador	1(7 meses – 5h/semana)	R$90,00	R$12.600,00
Co-Orientador	1(7 meses – 1h/semana)	R$90,00	R$2.520,00
Equipamento e Material Permanente			
Computador com TPM	2	R$3.200,00	R$6.400,00
Total			R$40.360,00

Item a ser adquirido	Computador com monitor, teclado e mouse.	
Tipo de contrato	Compra	
Documentos de aquisição (DT, etc.)		
Critérios de seleção de fornecedores (Critério e peso)	Critério	Peso
	Preço	Alto
Requisitos adicionais, premissas, restrições etc.	Computador deve ter TPM. HD de 500gb. 4Gb de memória. Monitor de 23”	
Processo de gerenciamento do fornecedor		
Papeis/responsabilidades no processo de aquisição	Papel	Responsabilidade
	Gerente do Projeto	Compra

5. Recursos Humanos

RH/ Stakeholders	Papel	Atuação	Instrução
Empresa Contratante	Dono do Projeto	Financiamento	-
	Cliente	Informar Requisitos	-
Orientador	Gerente do Projeto	Cobranças de Prazo	Ciência da Computação
	Avaliador Científico	Avaliação e Orientação	Ciência da Computação
Banca	Avaliador Científico	Avaliação e Orientação	Ciência da Computação
Gabriel	Gerente do Projeto	Planejamento	INE5427
	Pesquisador	Desenvolvimento do TCC	Ciência da Computação
	Programador	Documentação e desenvolvimento	Ciência da Computação
	Testador	Teste	-
Coordenador de Projetos	Coordenador de projetos	-	Ciência da Computação

6. Comunicação

O que precisar ser comunicado	Para quem	Forma de comunicação	Responsabilidades	Quando e com que freqüência
Status	Orientador	Via comunicação informal.	Orientando	Semanalmente
Status	Empresa Contratante	Via comunicação escrita formal.	Orientador	Mensalmente
Relatório parcial.	Orientador, Coordenador de projetos, Banca avaliadora	Via comunicação escrita formal.	Orientando	Uma Vez
Relatório final.	Orientador, Coordenador de projetos, Banca avaliadora	Via comunicação escrita formal.	Orientando	Uma Vez
Apresentação do relatório final.	Orientador, Banca avaliadora	Via comunicação oral formal.	Orientando	Uma Vez

Restrição da comunicação ou suposições:

A comunicação de status para o Orientador deverá ser realizada dentro do horário agendado pelo Orientador. Se necessário serão utilizadas outras formas de comunicação: e-mail, Skype, dentre outros.

7. Riscos

Risco	Probabi-lidade	Impacto	Prioridade	Estraté-gia de resposta	Ações de prevenção	Plano de contingência (definindo gatilho e ações)
Indisponibilidade de infraestrutura	Média	Alto	Alta	Aceitar	Já foram solicitados os equipamentos a empresas parceiras.	A empresa contratante deve prover os dispositivos.
Bibliotecas pouco conhecidas	Média	Alto	Média	Aceitar	-	Entrega de uma versão parcial, sem suporte ao dispositivo com problemas na biblioteca, e geração de um novo milestone com prazo maior.
HD queimar	Baixa	Baixo	Baixa.	Aceitar.	Realizar backup diário em um HD para backup.	Usar backup.
Doença	Baixa	Baixo	Baixa	Aceitar.	-	Continuar trabalhando.
Viagem	Baixa	Baixo	Baixa	Mitigar	Planejamento da agenda com antecedência.	Continuar trabalhando.