

Software para armazenamento de senhas desenvolvido em Java e MySQL com criptografia e utilizando o padrão MVC.

1st Bernardo de Souza Viero
Universidade Franciscana - UFN
Santa Maria - RS, Brazil
bernardo.viero@ufn.edu.br

2nd Herysson Rodrigues Figueiredo
Universidade Franciscana - UFN
Santa Maria - RS, Brazil
herysson.figueiredo@ufn.edu.br

Abstract—The main objective of this article is to guide and explain in a simple way how the development of the tool was carried out and thought out.

Index Terms—vault, mysql, criptografia

I. INTRODUÇÃO

O desenvolvimento de uma ferramenta para armazenamento de senhas, tornando-as mais seguras e mais simples de serem acessadas. Uma vez que diversas pessoas utilizam de bloco de notas para salvar suas senhas, o que gera uma grande insegurança. Além da insegurança também há o risco de perda dessas senhas.

Com isso, o desenvolvimento de uma ferramenta em Java que utiliza de uma Criptografia forte para o armazenamento de senhas no banco de dados tornando-as seguras e praticamente fazendo com que elas existam para sempre, uma vez que estarão rodando em um servidor seguro.

II. JAVA

A. Utilização de Java para criação da ferramenta

Java é uma linguagem Orientada a Objetos muito poderosa e com uma sintaxe bem comum, o que a torna fácil de resolver problemas utilizando-se da lógica de programação. É uma linguagem desenvolvida na década de 90 por uma equipe de programadores chefiada por James Gosling, na empresa Sun Microsystems, que em 2008 foi adquirido pela empresa Oracle Corporation.[2]

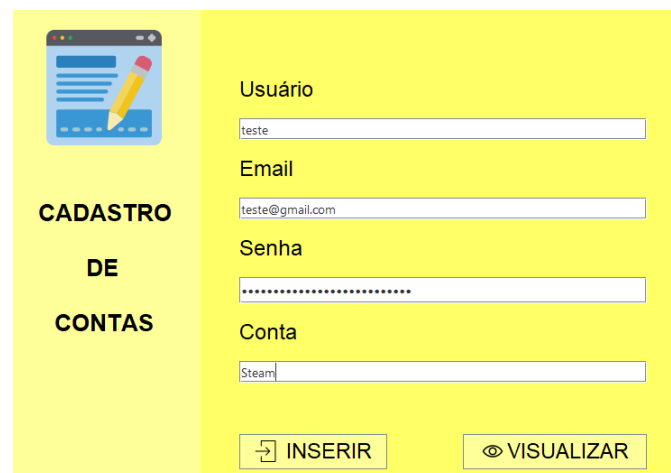
Diferente das linguagens de programação modernas, que são compiladas para código nativo, Java é compilada para um bytecode que é interpretado por uma máquina virtual (Java Virtual Machine, JVM). Conhecida como a mãe das linguagens e com mais de 30 anos de existência possui uma grande gama de bibliotecas o que torna mais fácil a vida do desenvolvedor na hora de construir a ferramenta desejada.

B. JFrame interface do software

Utilizou-se para o desenvolvimento Frontend da ferramenta o framework Swing conhecido como JFrame. Swing é um widget toolkit GUI (Interface de Usuário Gráfica) para uso com o Java. Ele é compatível com o Abstract Window Toolkit.

A API Swing procura renderizar/desenhar por conta própria todos os componentes, ao invés de delegar essa tarefa ao sistema operacional, como a maioria das outras APIs de interface gráfica trabalham.

Por ser uma API de mais alto nível, ou seja, mais abstração, menor aproximação das APIs do sistema operacional, ela tem bem menos performance que outras APIs gráficas e consome mais memória RAM em geral. Porém, ela é bem mais completa, e os programas que usam Swing têm uma aparência muito parecida, independente do Sistema Operacional utilizado. Além de possuir diversas personalizações fazendo com o que a interface gráfica fique da maneira com que o desenvolvedor achar mais interessante.[6]



A interface de registro de senhas é exibida em um fundo amarelo. À esquerda, há um ícone de um bloco de notas com uma caneta e o texto "CADASTRO DE CONTAS" em negrito. À direita, há um formulário com os seguintes campos: "Usuário" (com o texto "teste"), "Email" (com o texto "teste@gmail.com"), "Senha" (mascarado com pontos) e "Conta" (com o texto "Steam"). Abaixo dos campos, há dois botões: "INSERIR" com um ícone de seta para cima e "VISUALIZAR" com um ícone de olho.

Fig. 1. Tela de registro das senhas.

C. Modelo MVC

Para a construção do software utilizou-se o o padrão MVC. Ele é utilizado em muitos projetos devido a arquitetura que possui, o que possibilita a divisão do projeto em camadas muito bem definidas. Cada uma delas, o Model, o Controller e a View, executa o que lhe é definido e nada mais do que isso.

A utilização do padrão MVC traz como benefício o isolamento das regras de negócios da lógica de apresentação, que é a interface com o usuário. Isto possibilita a existência de várias interfaces com o usuário que podem ser modificadas sem a necessidade de alterar as regras de negócios, proporcionando muito mais flexibilidade e oportunidades de reuso das classes.[5]

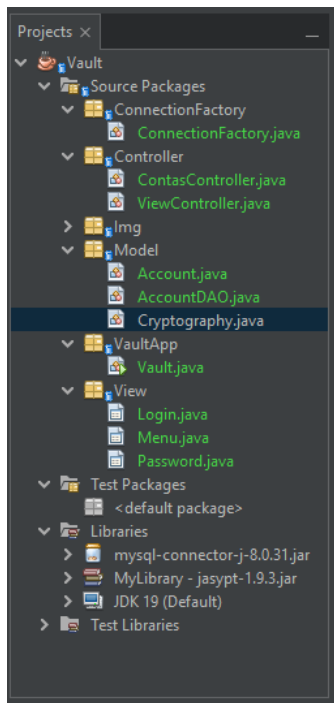


Fig. 2. Projeto utilizando o padrão MVC.

III. MYSQL

O MySQL é um sistema de gerenciamento de banco de dados (SGBD), que utiliza a linguagem SQL (Linguagem de Consulta Estruturada) como interface. É atualmente um dos sistemas de gerenciamento de bancos de dados mais populares da Oracle Corporation. Foi escolhido de para a utilização por ser um SGBD simples, e bem conhecido. Possui uma estruturação simples e de fácil entendimento, além de possuir uma grande segurança, e ser um banco de dados compacto para o desenvolvimento da nossa aplicação.[1]

Field	Type	Null	Key	Default	Extra
id_conta	int	NO	PRI	NULL	auto_increment
plataforma	varchar(50)	YES		NULL	
email	varchar(50)	YES		NULL	
usuario	varchar(40)	YES		NULL	
senha	varchar(50)	YES		NULL	

Fig. 3. Estrutura do banco de dados

IV. CRIPTOGRAFIA

A criptografia refere-se à construção e análise de protocolos que impedem terceiros, ou o público, de lerem mensagens

privadas. Muitos aspectos em segurança da informação, como confidencialidade, integridade de dados, autenticação.

A criptografia moderna existe na interseção das disciplinas de ciência da computação, engenharia elétrica, ciência da comunicação e física. Aplicações de criptografia incluem comércio eletrônico, cartões de pagamento baseados em chip, moedas digitais, senhas de computadores e comunicações militares.[4]

Para isso, tornou-se fundamental utilizar de uma Criptografia forte e de alta confiabilidade, para o armazenamento dessas senhas no banco de dados.

A. Biblioteca Jasypt

Jasypt é uma biblioteca java que permite ao desenvolvedor adicionar recursos de criptografia em seus projetos com o mínimo de esforço e sem a necessidade de ter um conhecimento profundo de como a criptografia funciona. Mas claro, além de fácil, o jasypt é altamente configurável. Você poderá escolher algoritmos de criptografia, geração de sal, geração de vetores de inicialização e muitos outros recursos avançados.[3]

Para o desenvolvimento do software utilizamos a classe Basic Text Encryptor que possui uma criptografia aleatória e que necessita de uma chave para a criptografia dos textos e a mesma chave para a descriptografia desses textos. Possui uma sintaxe bem simples, mas bastante poderosa e útil para o nosso sistema.

```
run:
Senha: testando criptografia
Criptografada: 4t3ppBBhu67KLAtyNkYlyTDQN+9sBVKKipC8pYGwa20ISYSxuyFHA==
Descriptografando a senha: 4t3ppBBhu67KLAtyNkYlyTDQN+9sBVKKipC8pYGwa20ISYSxuyFHA==
Temos: testando criptografia
BUILD SUCCESSFUL (total time: 0 seconds)
```

Fig. 4. Exemplo da criptografia utilizada

REFERENCES

- [1] MySQL "Documentação do MYSQL" Dez. 2022. [Online]. Available: <https://dev.mysql.com/doc/>
- [2] Java "Documentação do Java" Dez. 2022. [Online]. Available: <https://www.oracle.com/java/technologies/javase-documentation.html>
- [3] Biblioteca JasyPT "Documentação e modos de utilizar a biblioteca" Dez. 2022. [Online]. Available: <http://www.jasypt.org/>
- [4] Criptografia "Para que serve a Criptografia e por que devemos utiliza-la em nossos códigos" Dez. 2022. [Online]. Available: <https://aws.amazon.com/pt/what-is/cryptography/>
- [5] MACORATTI, J.C. "Padrões de projetos. 2010. O modelo MVC – Model View Controller." Dez. 2022. [Online]. Available: http://www.macoratti.net/vbn_mvc.htm/