Universidade Federal de Viçosa
Instituto de Ciência Exatas e Tecnológicas
CCF 355 - Sistemas Distribuídos e Paralelos

Trabalho 01

Gemmarium

Grupo:
Henrique de Souza Santana Matrícula: 3051
Pedro Cardoso de Carvalho Mundim Matrícula: 3877

Professor:
Thais Regina de Moura Braga Silva

18 de maio de 2022

1 Descrição Geral

O nome do sistema é Gemmarium, e se trata, de certa forma, de um jogo social de colecionamento de gemas mágicas virtuais. Essas gemas podem ser obtidas de duas maneiras: adquirindo de um servidor do jogo, ou trocando diretamente com outro usuário. Essas duas maneiras podem ser combinadas através de um mecanismo de fusão, que ocorre quando dois usuários trocam suas gemas e solicitam ao sistema que querem tentar fundir aquelas gemas trocadas em uma nova gema. A motivação do "jogo" está em descobrir novas gemas através de interações com o servidor e com outros usuários.

Podemos projetar quatro papéis nessa arquitetura: os Clientes, e três serviços - o Cofre, a Forja e a Galeria - compondo o sistema. Os Clientes podem comunicar entre si de forma par-a-par, e podem também comunicar com os três serviços do sistema. Todos tem pares de chaves pública e privada, e os três serviços são entidades confiáveis.

Pra cadastrar no sistema, um Cliente vai criar nome de usuário e senha com o Cofre, e informar também ao Cofre a sua chave pública. O Cofre então registra essas informações e notifica à Forja e à Galeria o nome desse novo usuário e a chave pública dele.

Para obter novas gemas, um Cliente deve comunicar com a Forja. A Forja vai identificar esse usuário, e entregar uma (ou mais) nova(s) gema(s) pra ele caso esteja dentro da cota do usuário (por exemplo, 1 pedido por dia). Essa mensagem é composta por todos os dados que representam aquela gema, junto de uma assinatura da Forja. Essa assinatura é uma mensagem criptografada pela chave privada da Forja, e contém: um ID da Forja, um ID do usuário que solicitou a gema, um ID da gema, um número aleatório, e a timestamp da criação da gema. Os dados da gema e a assinatura são criptografados em conjunto usando a chave pública do Cliente solicitante, e então enviada pra ele.

Todo Cliente pode comunicar com a Galeria e cadastrar o nome das gemas que possui, sem fornecer os dados completos das gemas. Assim, outros Clientes podem buscar na Galeria por Clientes que possuem alguma gema de seu interesse, e obter o IP desse outro Cliente.

Tendo o IP de um Cliente B, o Cliente A pode solicitar uma troca, listando o nome de quais gemas ele oferece e quais ele tem interesse. O Cliente B vê esse pedido e faz o mesmo, lista quais ele vai oferecer e quais ele tem interesse. Ao confirmar a troca, Cliente A criptografa os dados da gema junto à respectiva assinatura da Forja com a chave de B, e B faz o mesmo, com a chave de A, e os dados são trocados. Após a troca, ambos podem verificar a autenticidade das gemas usando a chave pública da Forja, e podem descartar gemas fraudadas.

Se ambos os Clientes permutantes estiverem interessados, eles podem solicitar uma fusão à Forja, que consiste em testar se há um conjunto de gemas compartilhadas pelos dois Clientes permutantes que se combinadas geram uma nova gema. Ambos Clientes enviam os dados das gemas para a Forja, a Forja verifica a autenticidade das gemas, e busca por uma fusão disponível. Se houver alguma fusão disponível, a Forja vai assiná-la da mesma forma descrita antes, porém colocando o ID de ambos os Clientes, e então entregar os dados da nova gema para ambos.

Além de poder verificar a autencidade das gemas, os usuários podem ver quem foram o usuários que descobriram aquela gema inicialmente através da assinatura da Forja, ou quais foram os usuários que se uniram para fundir uma gema, caracterizando o aspecto social do jogo.

1.1 Observações

1.1.1 Identificação de usuários

Para identificar um usuário sem pedir a senha, o servidor gera um número aleatório e criptografa com a chave pública do Cliente, e envia. O Cliente descriptografa com a chave privada dele, e criptografa com a chave pública do servidor, e responde. O servidor descriptografa e confere se o número casa com o que foi enviado, se sim, ele tem certeza que quem comunicou

com ele é alguém que possui a chave privada do Cliente em questão, e usa a chave pública do Cliente para identificá-lo no seu registro.

1.1.2 Troca de itens P2P

Não há necessidade dos Clientes apagarem os dados da gema que estão oferecendo, pois os usuários estão coletando *informação*, e não quantidades de itens físicos. Um problema da troca P2P, no entanto, é que não há garantia de que um Cliente vai cumprir com sua proposta, mas pelo menos, por não haver perda do que já se tinha, ninguém sai no prejuízo. No máximo, um Cliente não vai obter nenhuma gema (autêntica) nova.

1.2 Funcionalidades opcionais

Poderia ser interessante ter mais de uma Forja, que ofereça gemas diferentes de acordo com algum tema, o que incentivaria os usuários a buscarem fontes diferentes de gemas. Além disso, o Cofre poderia servir para relizar "backup" dos dados das gemas de cada Cliente, visto que o armazenamento dos dados das gemas é feito localmente.

2 Requisitos Funcionais

- **RF01:** O sistema deve permitir o cadastro de usuários usando nome de usuário e senha.
- **RF02:** O sistema deve reconhecer a identidade de um usuário utilizando seu login com nome e senha, ou através de um esquema de criptografia assimétrica.
- **RF03:** Cada usuário do sistema possui uma **coleção** de gemas.
- **RF04:** O sistema deve permitir que usuários solicitem novas gemas sorteadas para serem adicionadas à sua coleção, de acordo com uma certa cota de solicitações por usuário.
- **RF05:** O sistema deve permitir que os usuários registrem publicamente *o nome* das gemas estão dispostos a oferecer, e *o nome* das gemas nas quais tem interesse em obter. Esse registro é chamado de **galeria**.
- **RF06:** O sistema deve permitir que usuários naveguem pelas **galerias** de outros usuários.
- **RF07:** O sistema deve permitir a filtragem de **galerias** de demais usuários através do nome do usuário ou nome de gema.
- **RF08:** O sistema deve permitir a troca par-a-par entre usuários, na qual um dos usuários inicia uma proposta de troca a outro usuário, declarando quais gemas pretende oferecer, e em quais gemas possui interesse.
- **RF09:** O sistema deve notificar o usuário de novos pedidos de troca, permitindo que o mesmo responda também declarando quais gemas pretende oferecer, e em quais gemas possui interesse.
- **RF10:** O sistema deve permitir que qualquer usuário permutante decida rejeitar ou aceitar a troca, enviando os dados completos das gemas declaradas oferecidas para o outro usuário caso afirmativo.
- **RF11:** O sistema deve conhecer uma lista de conjuntos de gemas que, ao serem trocadas, podem gerar uma nova gema. Esse mecanismo de geração de gemas é denominado **fusão**.
- **RF12:** O sistema deve permitir, se ambos os usuários permutantes assim desejarem, tentar realizar uma **fusão** entre as gemas trocadas. A fusão ocorre apenas se cada usuário permutante possui pelo menos uma das gemas de algum conjunto de fusão válido.
- **RF13:** O sistema deve permitir que o usuário verifique a autenticidade das gemas de sua coleção, ou seja, verificar se foi obtida inicialmente através de alguma interação legítima com o sistema.
- **RF14:** O sistema deve permitir que o usuário apague gemas de sua coleção.

3 Diagrama de Casos de Uso

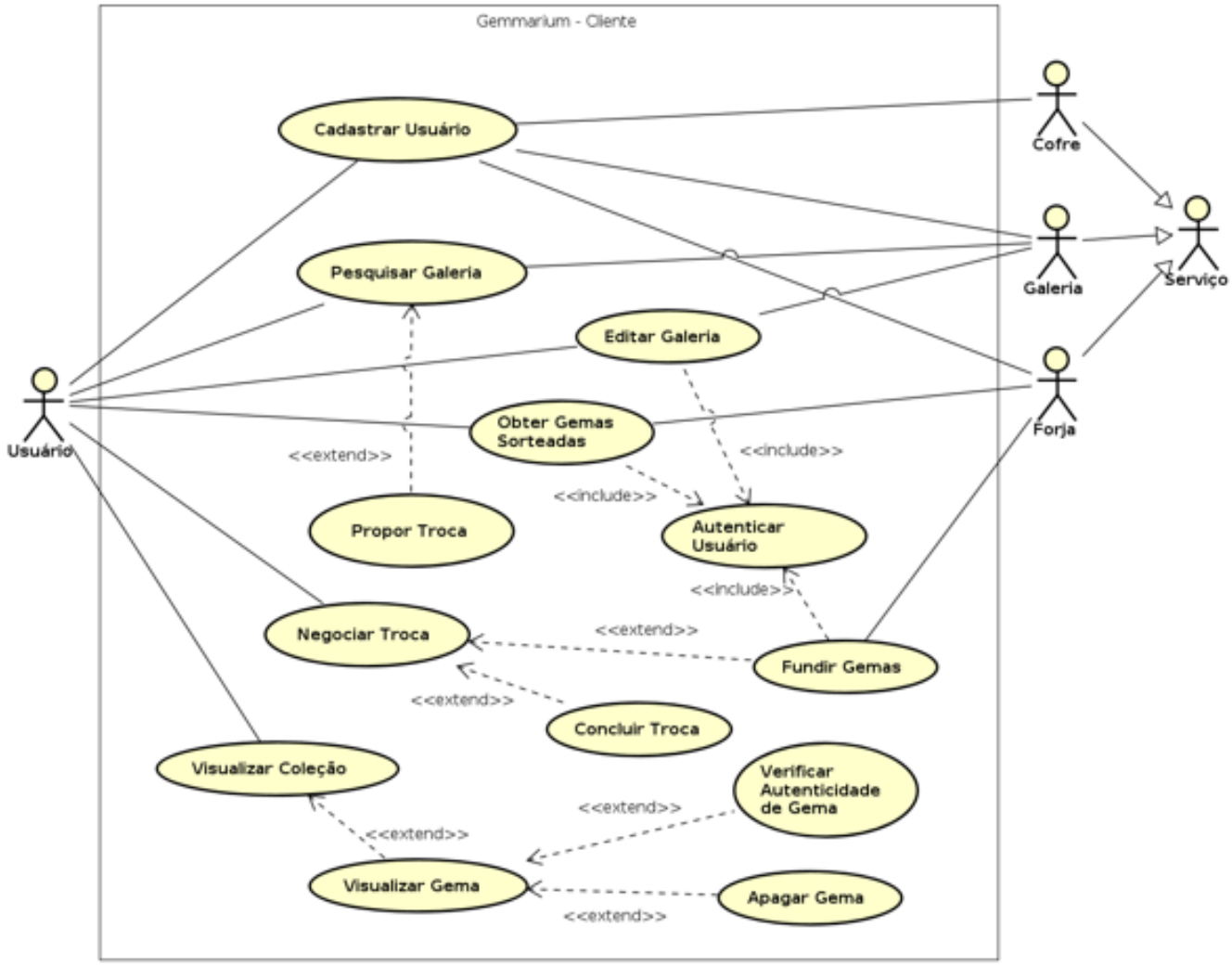

Figura 1: Diagrama de Casos de Uso.

4 Casos de Uso

Todos os casos de uso serão descritos do ponto de vista da aplicação Cliente, tendo o usuário como ator primário e as partes do sistema (Cofre, Forja e Galeria) como atores secundários, para facilitar o entendimento.

4.1 CSU01: Cadastrar Usuário

Sumário: O usuário utiliza o sistema para cadastrar sua identidade nos Serviços.
Ator primário: Usuário.
Atores secundários: Cofre, Forja e Galeria.

4.1.1 Fluxo principal:

1. O sistema apresenta uma página inicial com os campos de entrada para nome de usuário e senha.
2. O Usuário insere as credenciais escolhidas.
3. O sistema cria um par de chaves e envia ao Cofre as credenciais e sua chave pública.
4. O Cofre notifica a Forja e a Galeria do registro de um novo usuário, enviando a chave pública do mesmo.
5. O sistema redireciona para a tela de autenticação.
6. O sistema encerra o caso de uso.

Pós-condições: o Usuário foi cadastrado no Cofre.

4.2 CSU02: Visualizar Coleção

Sumário: O Usuário visualiza sua própria coleção de gemas.
Ator primário: Usuário.

4.2.1 Fluxo Principal:

1. O sistema apresenta a tela principal ao usuário.
2. O Usuário acessa a opção de visualizar sua coleção de gemas.
3. O sistema apresenta os dados de todas as gemas que o Usuário possui.
4. O sistema encerra o caso de uso.

4.3 CSU03: Visualizar Gema

Sumário: O Usuário visualiza os dados de uma gema específica de sua coleção.
Ator primário: Usuário.

4.3.1 Fluxo Principal:

1. O sistema apresenta a tela principal ao usuário.
2. O Usuário acessa a opção de visualizar sua coleção de gemas.
3. O sistema apresenta os dados de todas as gemas que o Usuário possui.
4. O Usuário seleciona uma gema.
5. O sistema exibe todos os dados daquela gema.
6. O sistema encerra o caso de uso.

4.4 CSU04: Obter Gemas Sorteadas

Sumário: O Usuário obtém novas gemas sorteadas.
Ator primário: Usuário.
Ator secundário: Forja.

4.4.1 Fluxo Principal:

1. O sistema apresenta a tela principal.
2. O Usuário solicita novas gemas sorteadas.
3. *Include* CSU13: Autenticar Usuário.
4. A Forja sorteia novas gemas e as assina para o usuário, enviando seus dados.
5. O sistema armazena os dados recebidos localmente e os apresenta para o Usuário.
6. O sistema encerra o caso de uso.

4.4.2 Fluxo de Exceção (4) - Cota excedida:

- Caso o Usuário tenha excedido a cota de solicitações de novas gemas, a Forja informa essa violação, além do tempo deve ser esperado para realizar uma nova solicitação.
- O sistema apresenta o erro, redireciona para a tela principal, e encerra o caso de uso.

Pós-condições: novas gemas aleatórias foram adicionadas à coleção do Usuário.

4.5 CSU05: Editar Galeria

Sumário: o Usuário edita suas gemas possuídas e de interesse na Galeria.
Ator primário: Usuário.
Ator secundário: Galeria.

4.5.1 Fluxo Principal:

1. O sistema apresenta a tela principal.
2. O Usuário solicita editar seus dados na Galeria.
3. *Include* CSU13: Autenticar Usuário.
4. O sistema solicita o estado atual da Galeria.
5. A Galeria informa os nomes das gemas que constam para aquele usuário.
6. O sistema apresenta o estado atual da Galeria ao Usuário, permitindo-o marcar ou desmarcar suas gemas possuídas, e também permitindo-o alterar a listagem das gemas de interesse.
7. O Usuário faz as alterações desejadas.
8. O sistema envia à Galeria a nova listagem de nomes de gemas.
9. A Galeria atualiza as informações, registrando também o IP daquele usuário.
10. O sistema encerra o caso de uso.

Pós-condições: a Galeria foi atualizada com base nas alterações feitas.

4.6 CSU06: Pesquisar Galeria

Sumário: O Usuário tenta encontrar outros usuários, de acordo com os critérios desejados.
Ator primário: Usuário.
Ator secundário: Galeria.

4.6.1 Fluxo Principal:

1. O sistema apresenta a tela principal.
2. O Usuário solicita buscar na Galeria.
3. O sistema apresenta uma caixa de buscas por nome de usuário ou por nome de gema. No caso da filtragem por nome de gema, o sistema também permite marcar se a busca é por gemas possuídas ou gemas interessadas.
4. O Usuário digita o termo que deseja buscar e confirma a busca.
5. O sistema envia essa solicitação à Galeria
6. A Galeria busca por usuários que se encaixam nos parâmetros de busca, e responde com esses dados, incluindo o IP de cada usuário para que possa ser localizado na rede.
7. O sistema apresenta ao Usuário os dados retornados pela Galeria.
8. O sistema encerra o caso de uso.

4.7 CSU07: Propor Troca

Sumário: O Usuário propõe uma troca com outro usuário.
Ator primário: Usuário.

4.7.1 Fluxo Principal:

1. O Usuário busca pela galeria de um outro usuário e solicita propor uma troca.
2. O sistema apresenta a coleção do Usuário.
3. O Usuário seleciona quais gemas de sua coleção ele deseja oferecer na troca, e confirma.
4. O sistema volta para a galeria do outro usuário.
5. O Usuário seleciona quais gemas do outro usuário ele possui interesse na troca, e confirma.
6. O sistema apresenta um campo de texto, um botão para submeter a solicitação de troca, e um botão de cancelar.
7. O Usuário insere uma mensagem que deseja enviar ao outro usuário junto com a solicitação de troca.
8. O sistema envia a solicitação de troca ao outro usuário através do IP encontrado na busca.
9. O sistema encerra o caso de uso.

Pós-condições: a solicitação de troca foi enviada e ficou como pendente para o outro usuário.

4.8 CSU08: Negociar Troca

Sumário: O Usuário dá prosseguimento à negociação da troca com outro usuário.
Ator primário: Usuário.
Precondições: Existe(m) troca(s) pendente(s) para o Usuário.

4.8.1 Fluxo Principal

1. Na tela principal, o sistema apresenta as solicitações de troca pendentes para o Usuário.
2. O Usuário seleciona uma solicitação de troca.
3. O sistema apresenta o estado atual da negociação, exibindo as mensagens trocadas entre os usuários, e as listas de nomes de gemas que cada um está disposto a oferecer e em quais tem interesse.
4. O Usuário pode escrever novas mensagens ao outro usuário ou também editar sua lista de gemas ofertadas/interessadas.
5. O sistema envia cada mensagem ou alteração para o outro usuário.
6. O sistema encerra o caso de uso.

Pós-condições: O estado da negociação da troca foi alterado, tendo adicionado novas mensagens ou atualizado as listas de gemas.

4.9 CSU09: Concluir Troca

Sumário: O Usuário aceita ou rejeita uma troca com outro usuário, encerrando-a.
Ator primário: Usuário.
Precondições: Existe(m) troca(s) pendente(s) para o Usuário.

4.9.1 Fluxo Principal

1. O Usuário está visualizando uma troca em aberto.
2. O Usuário aceita a troca.
3. O sistema envia todos os dados das gemas oferecidas para o outro usuário.
4. O sistema encerra o caso de uso.

4.9.2 Fluxo Alternativo (2): Usuario rejeita a troca.

- Caso o Usuário rejeite a troca, o sistema notifica o outro usuário da rejeição, apaga a proposta de troca e encerra o caso de uso.

Pós-condições: A troca foi rejeitada ou aceita, e no segundo caso, as gemas oferecidas foram enviadas ao outro usuário.

4.10 CSU10: Fundir Gemas

Sumário: O Usuário tenta realizar uma fusão entre as gemas sendo trocadas.
Ator primário: Usuário.
Ator secundário: Forja.
Precondições: Existe(m) troca(s) pendente(s) para o Usuário.

4.10.1 Fluxo Principal:

1. O Usuário está visualizando uma troca em aberto.
2. O Usuário decide tentar uma fusão entre as gemas que estão sendo oferecidas na proposta de troca.
3. O sistema notifica ao outro usuário que uma fusão está sendo tentada.
4. O sistema envia a solicitação de fusão à Forja, informando com quem a fusão está sendo tentada, e enviando os dados das gemas que está oferecendo.
5. *Include* CSU13: Autenticar Usuário.
6. A Forja recebe a solicitação e aguarda a mesma solicitação do outro usuário.
7. Caso ambas as solicitações estejam presentes, a Forja verifica a autencidade de todas as gemas envolvidas.
8. A Forja escolhe uma fusão disponível entre as gemas fornecidas pelos usuários, e envia os dados da gema resultante da fusão (caso haja), além das gemas trocadas pelos usuários aos seus respectivos destinatários.
9. O sistema recebe as gemas e encerra a proposta de troca como aceita.
10. O sistema encerra o caso de uso.

4.10.2 Fluxo de exceção (8): Gemas fraudadas.

- Caso a Forja detecte que há gemas fraudadas na troca, um erro é enviado aos usuários.
- O sistema apresenta o erro ao Usuário e encerra o caso de uso, concluindo a troca como rejeitada.

Pós-condições: A troca foi aceita e as gemas foram devidamente trocadas, incluindo a gema resultante da fusão, se houver.

4.11 CSU11: Verificar Autenticidade de Gema

Sumário: O Usuário utiliza o sistema para se certificar da autenticidade de uma gema.
Ator primário: Usuário.

4.11.1 Fluxo Principal:

1. O Usuário está visualizando os dados de uma gema de sua coleção.
2. O Usuário solicita que a autenticidade daquela gema seja verificada.
3. O sistema usa a chave pública da Forja para verificar a assinatura associada àquela gema, e informa ao usuário se os dados são autênticos.
4. O sistema encerra o caso de uso.

4.12 CSU12: Apagar Gema

Sumário: O Usuário apaga uma gema de sua coleção.
Ator primário: Usuário.

4.12.1 Fluxo Principal:

1. O Usuário está visualizando os dados de uma gema de sua coleção.
2. O Usuário solicita que aquela gema seja apagada.
3. O sistema apaga os dados daquela gema.
4. O sistema encerra o caso de uso.

Pós-condições: a gema selecionada foi apagada da coleção do Usuário.

4.13 CSU13: Autenticar Usuário

Sumário: O usuário fornece credenciais para que seja identificado.
Ator primário: Usuário.
Atores secundários: Serviço.

4.13.1 Fluxo principal:

1. O usuário solicita uma interação com um Serviço.
2. O sistema envia uma solicitação a esse Serviço.
3. O Serviço gera um número aleatório, criptografa-o com a chave pública do usuário, e responde ao sistema.
4. O sistema descriptografa com sua chave privada e responde ao Serviço o número encontrado.
5. O Serviço confere se o número recebido casa com o número gerado, e identifica o usuário.
6. O sistema encerra o caso de uso.

Pós-condições: o Usuário foi identificado pelo Serviço.