

Projet MIF01: Eliza GPT

1. Présentation

Le projet *Eliza GPT* s'est fait dans le cadre de l'UE *Gestion de projet et génie logiciel* (MIF01). Ce projet a pour objectif de réaliser une petite application qui nous permet de discuter avec un chatbot du nom de "Eliza". Ce chatbot pourra répondre, de manière plus ou moins naturelle, aux différents messages que l'utilisateur écrira. Il est important de noter que nous sommes très loin de ce qu'est "ChatGPT" qui est une intelligence artificielle. Ce projet avait pour but de nous initier à ce qu'est la gestion de projet tel que nous pourrions la connaître plus tard en entreprise. Pour cela, nous avons travaillé en binôme en utilisant la forge de l'université et ces différentes fonctionnalités. De plus, le projet nous a aussi permis de découvrir et d'appliquer les designs patterns. Enfin, lors de ce projet, une phase de tests était aussi présente, les tests étant une partie importante de la gestion de projet en entreprise. Le langage de programmation qui a été utilisé est Java qui est un langage orienté objet et qui facilite l'utilisation des design pattern.

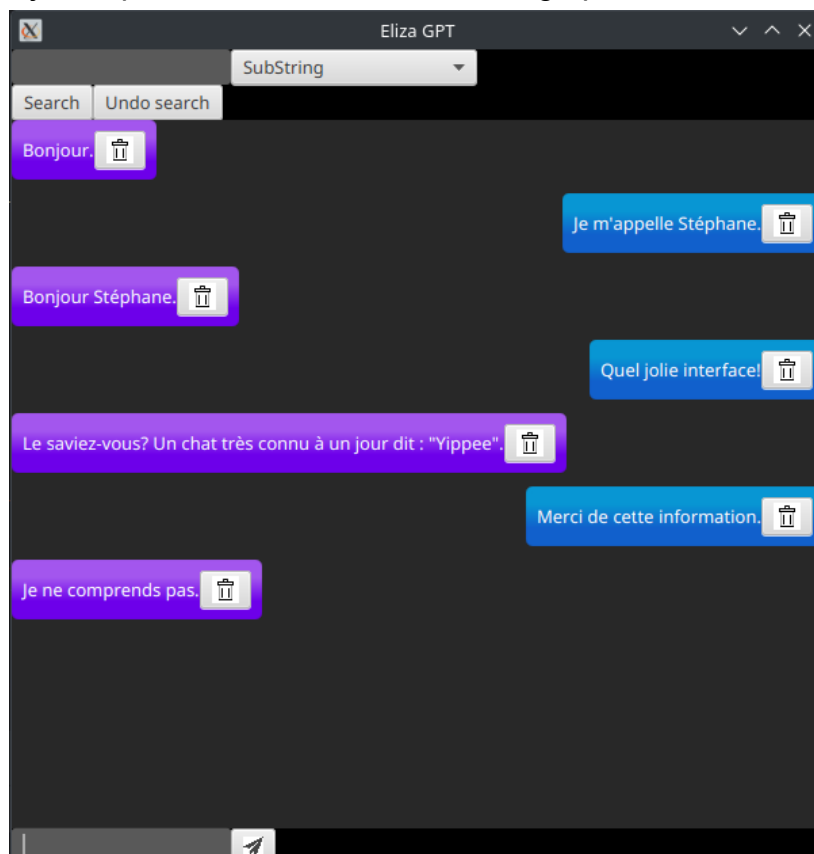


Figure 1 : Interface d'Eliza GPT.

2. Designs Patterns

Lors de ce projet, de nombreux designs patterns ont été utilisés afin de rendre le code de l'application plus sensé ainsi que plus modulable et enclin à la modification. En effet, les fonctionnalités se doivent d'être facilement modifiables pour qu'il soit possible dans le futur de rajouter une fonctionnalité sans avoir à modifier de nombreuses autres fonctionnalités. C'est pourquoi dans un premier temps, il a fallu appliquer le pattern MVC qui consiste à séparer le code en trois grandes parties. La première est la modèle, aussi appelée "partie métier". Le modèle contient toute la partie fonctionnelle et la logique de l'application. On y retrouve donc des fonctionnalités telles que la prise de décision de notre chatbot, la gestion des données, qui sont ici nos messages, et les différentes stratégies de recherches de messages. De plus, le modèle est complètement indépendant de la vue ainsi que du contrôleur. La deuxième partie du pattern MVC est la vue. C'est la partie en charge de l'affichage de notre application. La vue permet donc de faire le lien entre l'utilisateur et l'application. Elle a uniquement connaissance du contrôleur et aucune logique n'est présente. Enfin, le contrôleur est la dernière partie de notre pattern. Le contrôleur permet de faire le lien entre la vue ainsi que la logique de notre application. Ceci signifie que toutes les actions qui auront lieu au niveau de l'interface utilisateur seront transmises au contrôleur afin qu'il puisse appeler les bonnes fonctions de notre modèle. On en déduit que le contrôleur a connaissance de la vue ainsi que de la partie métier de l'application.

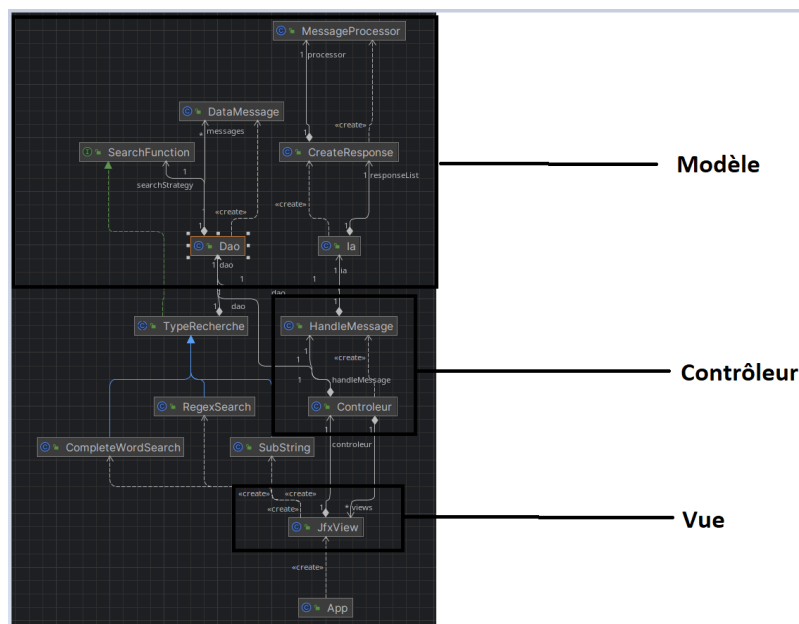


Figure 1 : Diagramme de notre application.

En plus du pattern MVC, d'autres designs patterns ont été appliqués durant ce projet. Tout d'abord, le pattern "singleton" a été utilisé lors de ce projet. Ce pattern permet de créer qu'une seule instance d'un objet qui sera commun à tout le

programme. C'est pourquoi, il a été décidé de l'utiliser à deux types d'objets. Le premier est le contrôleur. Ce n'était pas le cas au début du projet. Toutefois, il a été nécessaire d'appliquer le pattern singleton à cette classe pour que la synchronisation de la vue sur plusieurs fenêtres soit possible. La seconde classe qui est de la forme singleton est notre classe regroupant toutes les données de l'application. Cette classe étant un DAO (Data Access Object), il était capital qu'il ne puisse avoir qu'une seule et unique instance de cette structure dans notre projet. En effet, dans le cas contraire, la duplication ou la perte de données auraient été des événements possibles, ce qui aurait entraîné de graves conséquences. De plus, le DAO nous semblait être le pattern adéquat pour stocker les différentes données relatives à nos messages.

Dans notre vue, de nombreux callbacks ont été implémentés à l'aide, ou non, de lambda fonction. Ces callback ont pour but d'appeler des méthodes particulières du contrôleur lors de certaines actions. On peut notamment citer les callbacks présent sur les boutons de recherche qui permettent de déclencher la recherche en appelant le contrôleur.

Enfin, le pattern "Stratégie", couplé à des callbacks, nous a permis d'implémenter différents types de recherches, et ce, via une interface. Le pattern "Stratégie" à la particularité de rendre l'ajout d'une stratégie trivial. En effet, si nous souhaitons plus tard ajouter un nouveau type de recherche, il suffira de rajouter une nouvelle classe qui héritera de la classe TypeRecherche et qui réimplémentera la fonction de l'interface SearchFunction. Les callbacks quant à eux permettent tout simplement de changer la stratégie de recherche qu'emploie notre DAO. Le pattern stratégie aurait pu être utilisée pour deux autres fonctionnalités, mais nous n'avons pas eu le temps. La première fonctionnalité est celle de la création des réponses de l'IA. La seconde aurait été une fonctionnalité qui permettrait à notre vue de passer d'une UI à une autre en appuyant sur un bouton. Ce bouton aurait été équipé d'un callback qui appellerait une fonction issue d'une interface.

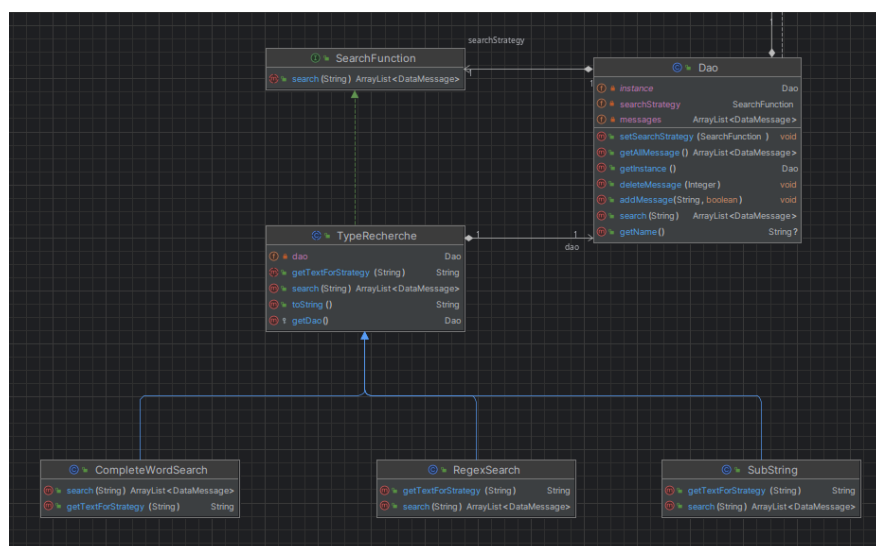


Figure 2 : Diagramme représentant le pattern "Stratégie" ainsi que le DAO.

3. TEST

Lors du développement d'ElizaGPT, une série complète de tests unitaires a été menée sur les composants clés du système : le modèle, le contrôleur et la vue. Ces tests visaient à garantir la fiabilité de l'application.

Les tests unitaires du modèle devaient vérifier l'intégrité de la logique métier que nous avons écrit. Pour cela, des tests sur les différentes classes de cette partie ont été écrits.

Les tests sur le contrôleur se sont avérés plus difficiles que le modèle. En effet, le contrôleur, étant la passerelle entre la logique de l'application et son interface utilisateur. Il était difficile de tester ces interactions. Toutefois, l'utilisation de la librairie Mockito a facilité la tâche en créant des scénarios.

Des scénarios ont aussi été utilisés afin de tester la vue. Il est cependant très difficile de faire des tests automatiques sur cette dernière.

4. L'Intelligence artificielle et l'éthique

Les intelligences artificielles ont connu une réelle avancée depuis quelques années. On peut notamment citer Midjourney, qui est spécialisé dans la génération d'images artistiques, GitHub Copilot, spécialisé dans la rédaction de code et enfin ChatGPT qui est une intelligence artificielle de génération de textes avec laquelle on peut converser. Parmi les intelligences artificielles citées, ChatGPT est de loin la plus connue. Dans cette partie, nous nous intéresserons à ce dernier type d'IA.

L'intelligence artificielle conversationnelle, représentée par des chatbots et des assistants virtuels, a des implications significatives et positives dans notre société. Ces systèmes assurent une accessibilité continue, réduisent les coûts opérationnels grâce à l'automatisation des tâches, et améliorent l'efficacité en libérant les équipes humaines pour des tâches plus complexes. En analysant les données utilisateur, ils personnalisent les interactions, contribuant ainsi à une expérience utilisateur enrichie. Leur adaptabilité universelle les rend pertinents pour des entreprises de toutes tailles, tandis que leur capacité à fournir des réponses rapides améliore la satisfaction client. De plus, la collecte de données permet une analyse pertinente pour orienter l'amélioration continue des produits et services. L'apprentissage continu des IA conversationnelles et leur facilitation de l'accès à l'information en font des catalyseurs d'innovation.

Toutefois, ces IA soulèvent de nombreux autres problèmes tels que la question du plagiat. Par exemple, le précédent paragraphe a été entièrement généré avec ChatGPT à l'aide des indications suivante : "Quels sont les avantages qu'octroie une IA conversationnelle à la société ?", "fais en sorte que ça ne soit pas une énumération" et "raccourcis le texte, fais en un paragraphe et vulgarise-le légèrement pour un projet universitaire". Cette question du plagiat était au centre de l'attention en début d'année 2023 à l'école supérieure Science Po Paris. En effet, de

fortes règles ont été établies sur l'utilisation de ChatGPT afin de réduire et de combattre le plagiat [1]. De plus, d'autres problèmes tels que la désinformation sont aussi causées par des IA conversationnelles. Lors d'un test effectué en ce début d'année 2023 par NewsGard, une société américaine luttant contre la désinformation. Il a été montré que la nouvelle version de ChatGPT (ChatGPT4) était plus encline à produire des fake news. Le test consistait à demander à ChatGPT 3.5 et 4 de créer de fausses informations. Il s'est révélé que la version antérieure produisait 80% des fausses informations alors que la dernière version en produisait pour chaque demande [2].

Afin de remédier à des risques tels que la désinformation, des mesures ont été adoptées. Dans un premier temps, un système d'autorégulation a été mis en place par OpenAi, la société derrière ChatGPT. Cependant, des lois sont déjà présentes afin de réguler ces IA, et ce, malgré leur récente effervescence. Il n'y a donc pas de vide juridique, car il est toujours possible de se référer à des textes de loi plus généraux. Malheureusement, un vrai flou juridique est quant à lui toujours présent. En effet, les IA génératrices s'appuient sur des bases de faits, ce qui fait que les informations utilisées doivent normalement être sourcées. L'Union européenne a rendu exceptionnelle la possibilité pour les IA d'utiliser des œuvres protégées afin d'entraîner les IA. Ceci est possible tant que les auteurs n'ont pas fait d'opposition. Toutefois, de l'autre côté du pacifique, aux États-Unis, cette décision est toujours au centre de débats. Pour ce qui est du texte ou image généré par l'IA, le problème est tout autre. Effectivement, il est assez difficile de savoir s'il y a eu, ou non, respect des droits d'auteurs puisque comme dit plus tôt, le texte et les images sont créés sur une base de faits qui s'appuie sur une multitude d'œuvres qu'il ne citera pas. Cependant, cet argument est aussi en faveur de l'intelligence artificielle. Puisqu'une quantité phénoménale d'information est utilisée afin d'obtenir un résultat, il peut s'avérer être complexe de parler de plagiat [3].

Ensuite, le respect des données fourni par l'utilisateur est capital. En effet, comme dit plutôt, les IA conversationnelles s'entraînent en s'appuyant sur des bases de données déjà présentes. De plus, dans le but de s'améliorer, les chatbots utilisent les différentes conversations que ce dernier a pu avoir avec les utilisateurs. Il est donc difficile pour le Règlement Général sur la Protection des Données (RGPD) de laisser chaque individu exercer les droits qu'il a sur ses données. Il est aussi important de noter que ChatGPT précise que la saisie d'informations confidentielles sur la plateforme est à éviter, car ces données risquent d'être utilisées pour améliorer le chatbot. Enfin, une réglementation sur l'IA en Europe est actuellement en projet dans le but de préciser certains points du RGPD.

Comme nous l'avons vu, de nombreuses réglementations sont en train d'être mises en place pour des IA. Cependant, Eliza GPT fait face à de nombreuses limites. Pour commencer, les réponses fournies par cette dernière sont très souvent peu pertinentes ou hors-sujet. Ceci est grandement dû au fait que le chatbot ne s'appuie pas sur une base de fait. Néanmoins, ceci implique que si des personnes mal intentionnées étaient derrière la création de l'application, elle pourrait très facilement en faire un créateur de fausses informations. Ils leur suffiraient de créer

de fausses informations qui seront envoyées à l'utilisateur s'il demande, par exemple, des informations sur l'actualité. De plus, tous les messages écrits par l'utilisateur sont stockés. Dans notre cas, ces informations sont perdues dès que l'application est fermée. Toutefois, ces données pourraient être sauvegardées sur un serveur, ce qui pourrait être dangereux si ces données sont critiques.

5. Bibliographie

[1] SciencePo. (2023, 27 janvier), SCIENCES PO INTERDIT SANS MENTION PAR L'ÉTUDIANT L'UTILISATION DE L'OUTIL CHATGPT. *SciencePo*.

<https://newsroom.sciencespo.fr/sciences-po-interdit-lutilisation-de-loutil-chatgpt/>

[2] La pointe, P. (2023, 22 mars), *La version 4 de ChatGPT et la désinformation : meilleure et améliorée*. Agence Science-Presse.

<https://www.sciencepresse.qc.ca/actualite/2023/03/22/version-4-chatgpt-desinformati-on-meilleure-amelioree>

[3] Malroux, E. (2023, 26 avril), [Dossier IA générative] - Quelles régulations pour la conception des IA génératives ? *Laboratoire d'Innovation Numérique de la CNIL*

<https://linc.cnil.fr/dossier-ia-generative-queelles-regulations-pour-la-conception-des-ia-generatives>