

Cahier des charges V0

Valar Morghulis
by
Birna G  rald & Sergent Pierre-Louis

15-06-2020

Contents

Introduction	3
Contexte	3
Demande	3
Enjeux	3
Description	4
Objectifs	4
Stockage <i>cloud</i> sécurisé	4
<i>Feed</i> d'actualité	4
Utilisateurs	5
Fonctionnalités principales	5
Scénario 1	5
Scénario 2	6
Réalisation	6
Critères d'acceptation	6
Contraintes	7

Introduction

Contexte

Organiser la liberté de la presse, protéger les lanceurs d'alerte est un enjeu démocratique à garantir pour nos sociétés. C'est un sujet brûlant de l'actualité.

Mais comment déjouer la propagande : pour que cette liberté s'exerce pleinement, si les sources doivent être protégées, elles doivent être aussi vérifiées.

Comment sauvegarder, authentifier, partager, soumettre à vérification des documents, des écrits, des photos, des vidéos sans mettre en danger le lanceur d'alerte.

Suite à l'affaire Snowden, plusieurs ébauches de solution ont été mises sur le marché (SecureDrop). Ces solutions s'appuient toujours sur le réseau de navigation anonymisé TOR.

Demande

On peut donc constater qu'il y a un réel besoin de protection et de sécurité pour ces gens, en reprenant l'affaire Snowden notamment, qui souhaitent dévoiler d'importantes informations dans l'intérêt commun sans s'exposer à des représailles.

Mais dans une moindre mesure toute personne qui souhaite faire valoir son droit de liberté d'expression, devrait pouvoir le faire sans passer par des réseaux anonymes tels que TOR.

On remarque aussi que de plus en plus de gens aiment s'informer par eux même, par le biais des réseaux sociaux. Cependant cela souvent au détriment de la véracité des propos.

Enjeux

Les enjeux seront donc multiples afin de répondre au mieux à la problématique suivante : “Comment **garantir la sécurité des lanceurs d'alertes**, et comment **garantir au grand public la véracité des informations fournies** ?”

Description

Objectifs

L'objectif principal de ce projet sera donc de mettre en place une plateforme web permettant de répondre aux problématiques énoncées auparavant.

Le site comportera deux modules principaux.

Stockage *cloud* sécurisé

Un espace de stockage *cloud* qui permettra aux utilisateurs de stocker des articles accompagnés de documents.

Ces données seront cryptées sur le serveur et seront lisibles uniquement avec un système de clefs. Ces articles pourront ensuite être mis à la disposition des médias (présent sur le site), qui vérifieront l'exactitude des informations.

Avec ce premier module on pourra donc établir un lien sécurisé entre les lanceurs d'alertes et les médias. Cette première partie sera donc plutôt portée sur la sécurisation des données et sur la relation lanceur d'alerte - média.

Les *news* ne seront pas publiées directement sur l'espace public du site, mais pourront être relayées par les médias après vérification (par leurs propres moyens). L'utilisateur peut quand même décider à tout moment de publier son article sur l'espace public du site, avec ou sans la validation des médias.

Feed d'actualité

Alors que la première partie met l'accent sur l'intervention d'un organisme tier afin de vérifier la véracité des informations postés, ce module aura un aspect plus communautaire.

Si certains utilisateurs veulent relayer des *news* moins sensibles, ils pourront alors rendre public l'information directement sur le site. Les médias présent sur la plateforme pourront toujours vérifier certaines informations, et auront un poids plus important sur la *réputation* du post.

Car en effet, les utilisateurs lambda pourront aussi contribuer à vérifier les *news* postés et ce de deux manières :

- Un système de upvote / downvote, à la manière de Reddit
- Une possibilité d'ajouter des sources (liens vers d'autres articles, livres, etc) confirmant ou infirmant les informations données (à la manière de Wikipédia)

Ainsi, sur des informations plus légères, les utilisateurs pourront contribuer à leur tour à la véracité des articles. Bien évidemment la vérification par ce biais est moins fiable, et le verdict des médias aura un poids prédominant.

Utilisateurs

La plateforme comportera deux types d'utilisateurs différents:

- **Utilisateur lambda / lanceur d'alerte:**

Il s'agit de l'utilisateur de base qui pourra consulter le fil d'actualité, contribuer sur les posts en ajoutant des sources, *upvoter* / *downvoter* des posts. Et surtout c'est lui qui pourra (de manière anonyme), créer de nouveaux articles pour ensuite les soumettre aux médias ou les publier directement.

- **Utilisateur vérifié / média:**

Il s'agit d'un média ou d'un journaliste agréé. C'est lui qui aura accès aux articles soumis par les utilisateurs lambda. Il pourra vérifier la véracité des informations avec un poids important. Il pourra aussi vérifier les articles postés publiquement, et ce de manière anonyme.

Fonctionnalités principales

Les fonctionnalités principales ont été quelque peu décrite auparavant. Nous allons donc prendre deux scénario pour mieux comprendre l'enchainement des actions.

Scénario 1

Louis est un passionné d'informatique et de développement, c'est pourquoi il a assisté à une conférence sur ReactJS la veille. Durant cette conférence il a appris une nouvelle majeure concernant son *framework* favori, il n'a pas vu d'article à ce propos et il décide donc de partager la nouvelle. Cependant il n'a pas pris de vidéo, il n'a donc aucune preuve de ce qu'il avance. Il décide donc de se rendre sur son site de *news* préféré : ***Valar Morghulis***.

Il y écrit un court article détaillant la nouveauté lié à ReactJS, et post directement l'article sur l'espace public du site. Quelques jours plus tard, il retourne sur la plateforme et constate qu'il a reçu plusieurs *upvote* ainsi que des collaborations pour confirmer ses dires. En effet, plusieurs personnes ont partagé des articles en rapport avec la nouveauté qu'il avait reporté, une personne était même présente à l'évènement et a pris une vidéo qu'elle a pu joindre au post.

Ainsi, Louis a pu lui même vérifier ses dires grâce aux articles communiqués par les autres utilisateurs, et l'information qu'il a communiqué a bénéficié directement à la communauté. De plus, la collaboration de la communauté a permis de confirmer la véracité de sa *news*.

Scénario 2

Pour ce second scénario on peut reprendre l'affaire Snowden (en atténuant certains points).

Edward Snowden, après des années de travaux pour la NSA, décide de dévoiler certaines pratiques de l'organisme qui vont à l'encontre des libertés individuelles et du respect de la vie privée. Il décide d'utiliser la plateforme **Valar Morghulis** pour sa discrétion et sa sécurité.

Il y crée alors un article, en joignant une grande quantité de fichiers pour appuyer ses propos. Ces fichiers sont hautement confidentiels, mais il sait que la plateforme crypte les données stockées, et qu'il n'a donc rien à craindre. Compte tenu de l'importance des informations, il va bien évidemment se garder de publier cela sur l'espace public.

En revanche, il va effectuer une sélection de journalistes et de médias grands publics, qui possèdent un compte vérifié sur la plateforme, afin de leur transmettre l'information de manière anonyme (directement sur la plateforme). Une fois cela réalisé, les médias vont ensuite valider la *news* et, suite à un accord, vont transmettre une partie de ces informations au grand public. Les médias décident aussi de tourner une vidéo où Snowden apparaît, pour rendre la nouvelle encore plus crédible aux yeux du monde. Bien évidemment, la vidéo est alors stockée en toute sécurité sur la plateforme.

Une fois que toutes les précautions ont été prises, que les vidéos ont été tournées et que tous les médias ont vérifié l'information, Edward Snowden décide de publier son article sur l'espace public du site. Il a ainsi pu, tout au long du processus, protéger ses données, et ajouter du poids à son propos en récoltant la vérification des différents médias.

Réalisation

Critères d'acceptation

Pour un tel projet on peut tenir compte des critères secondaires d'acceptations tels que : la **rapidité** et l'**ergonomie**, afin de garantir une expérience fluide.

Cependant le point le plus important sera de garantir un cryptage des données fonctionnel, afin de garantir **sécurité** et **fiabilité** (pas de perte de données par exemple).

Contraintes

- **Temps** : période de développement assez courte, possibilité de développer uniquement un des deux modules présentés (stockage).
- **Environnement de développement** : travail à distance, ne facilite pas la communication et la coordination des tâches.
- **Environnement technique** : la réussite du projet repose en grande partie sur la capacité de la plateforme à encrypter les données. Il s'agit d'une tâche critique qui n'est pas remplaçable, il sera donc important de se pencher sur la question dès le début du projet.