haute école neuchâtel berne jura arc ingénierie www.he-arc.ch

Hes·so Haute Ecole Spécialisée de Suisse occidentale

Attack detection with AI

Julien CHAPPUIS

Travail de Bachelor 2020

Informatique - Développement Logiciel et Multimédia

Professeur: Stefano CARRINO

Expert: Philippe KAPFER

Description

Ce travail de Bachelor a été proposé par l'entreprise NextDay Vision qui souhaite obtenir une étude de faisabilité sur le concept de sécurité qu'est l'authentification continue. Cette mesure consiste à authentifier l'utilisateur en permanence.

L'objectif de ce travail est donc d'effectuer des recherches et des expériences sur la thématique. Plus précisément, le but est de déterminer si le *machine learning* est un bon moyen de réaliser de l'authentification continue.

L'apprentissage du comportement clavier de l'utilisateur permet d'entraîner un modèle de type réseau de neurones capable de classifier si l'utilisateur est authentique ou un intrus.

Ce projet a aussi pour but de décortiquer la problématique et de faciliter le travail de l'équipe qui le continuera.

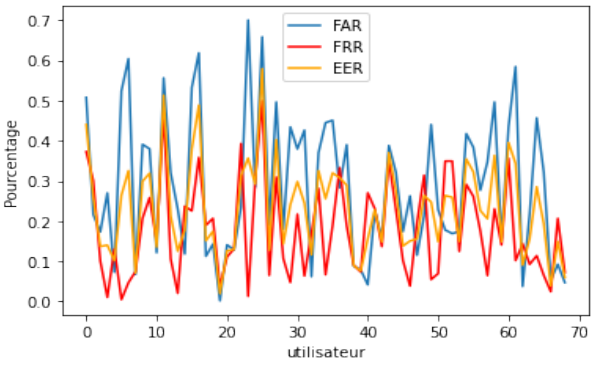
Déroulement

Ce travail de Bachelor s'est déroulé selon les étapes suivantes :

- Compréhension de la problématique.
- Analyse de l'état de l'art et recherche de publications similaires.
- Évaluation et choix de solutions potentielles à explorer.
- Prétraitement et analyse des données obtenues.
- Implémentation d'un modèle de type réseau de neurones.
- Entraînements de modèles et évaluation des performances obtenues.
- Identification et compréhension des jeux de données ayant obtenu de mauvais résultats.
- Amélioration du modèle et des données d'entrainement.
- Réalisation d'une application de démonstration.

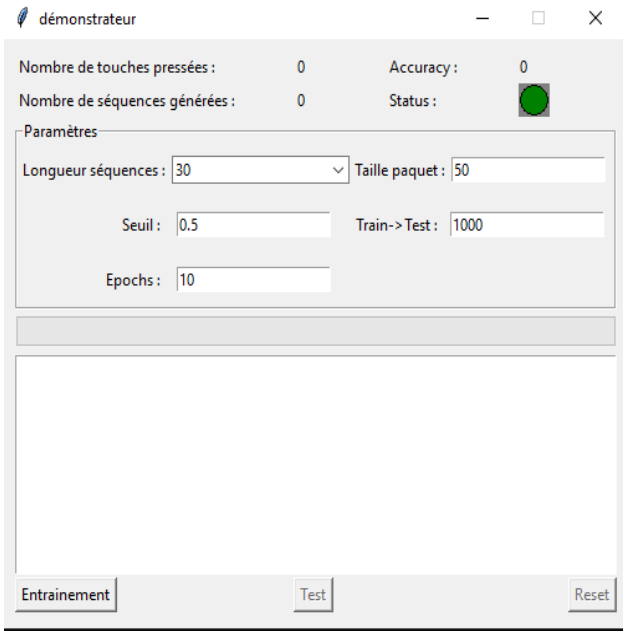
Résultats

Un réseau de neurones capable de détecter si un utilisateur est authentique a été mis en place et testé. De plus, diverses investigations ont permis de déterminer la source des mauvais résultats.



Performances par utilisateur. Plus le pourcentage est bas et plus l'utilisateur a un bon résultat.

Une application capable d'analyser le comportement clavier de l'utilisateur et d'indiquer visuellement lorsque celui-ci n'est pas authentique a été développée. Elle permet d'appliquer le concept dans un cas pratique.



Aperçu de l'interface graphique de l'application de démonstration

Perspectives

Les recherches et les tests réalisés ont prouvé que le *machine learning* arrive à répondre à la problématique de l'authentification continue. L'analyse d'autres sources de données telle que la souris permettrait d'améliorer la stabilité et les performances du système. Étant donné que c'est un projet de recherche, beaucoup de tests ont été effectués. L'ensemble du travail réalisé permettra à l'équipe continuant ce projet de partir sur de bonnes bases.