Authentification d'un utilisateur à partir de ses traces d'interaction

Fatma Derbel, Pierre-Antoine Champin, Amélie Cordier, Damien Munch

Authentification d'un utilisateur à partir de ses traces d'interaction

Fatma Derbel[1,2] Pierre-Antoine Champin[1] Amélie Cordier[1] Damien Munch[2]

[1] Université de Lyon, CNRS Université Lyon 1, LIRIS, UMR5205, F-69622, France
[2] Ignition Factory

fatma.derbel@liris.cnrs.fr

Résumé

Cet article [1] présente une démarche pour concevoir et implémenter un système d'authentification des utilisateurs dans les plates-formes web de formations certifiantes. Le système que nous proposons s'appuie sur deux modules : l'un combinant intelligemment différentes méthodes d'authentification connues, en fonction de leur disponibilité, et l'autre proposant une nouvelle approche d'authentification des utilisateurs à partir de leurs traces d'interaction. Ce système sera intégré dans la plate-forme de formation en ligne conçue et développée par la société Ignition Factory [2]. Dans cet article, nous présentons nos travaux préliminaires pour la définition de l'architecture de ce système, ainsi que l'état de l'art des méthodes d'authentification que nous avons réalisé.

Mots Clef

Authentification des utilisateurs, traces modélisées, environnements informatiques pour l'apprentissage humain, plates-formes de formation en ligne.

1 Introduction

Les plates-formes de formation en ligne sont de plus en plus répandues, notamment du fait du succès actuel des MOOCs (Massive Open Online Courses). On distingue deux types d'usage de ces plates-formes : d'une part la diffusion ouverte, massive et libre de contenus pédagogiques sur des sujets variés, et d'autre part, l'usage pour les formations certifiantes. Dans ce dernier cas, l'authentification des utilisateurs soulève des problèmes qui n'apparaissent pas souvent dans le cas général. Par exemple, lorsqu'il s'agit de leur compte en banque ou de leur compte sur un réseau social, les utilisateurs ont rarement intérêt à partager leurs éléments d'authentification (mot de passe, réponse à une question secrète, etc.). Quand bien même ils le feraient, ils seraient les seuls à devoir en assumer les conséquences. En revanche, dans le cas d'une formation certifiante, les utilisateurs pourraient être amenés à partager leurs éléments d'authentification pour frauder en vue de l'obtention de la certification. Du point de vue des organismes utilisant ces plateformes pour délivrer des certifications, la question de la fiabilité de l'authentification est donc cruciale car elle garantit la crédibilité des certificats délivrés. Cet article s'intéresse à la problématique de l'authentification d'apprenants dans le contexte des formations certifiantes en ligne. Plus précisément, nous cherchons à garantir avec un certain degré de confiance, et ce, tout au long de la formation, que c'est bien la même personne qui l'a suivie et validée. Nous cherchons donc à bâtir un système qui a les propriétés suivantes :

Le système est **indépendant du contexte matériel de l'apprenant** : nous ne faisons pas d'hypothèse forte sur la possibilité de l'apprenant à avoir accès à des dispositifs tels qu'une webcam, un lecteur d'empreintes digitales ou encore un micro. Le système permet **une authentification continue** : nous proposons une solution qui vérifie régulièrement l'identité de l'utilisateur, et ce, durant tout le processus de formation. Ce processus garantit un minimum d'interruptions de l'apprenant durant son activité.

Le système analyse en **temps réel** les comportements de l'utilisateur et déclenche **dynamiquement** des alertes en cas de comportements suspects. À leur tour, ces alertes déclenchent un mécanisme complémentaire d'authentification.

Le système permet une **combinaison de différente méthode d'authentification** (voir 2.1) selon leur disponibilité à la phase inscription.

Le système pourra utiliser **des mesures comportementales** pour déterminer l'identité de l'utilisateur en fonction d'une analyse de son comportement, capturé via ses interactions avec le système et via ses activités toute au long de la session d'apprentissage. Ces interactions peuvent en effet être capturer d'une manière continue, difficilement falsifiable et non intrusive. L'ensemble des informations de ces interactions peuvent donc créer un modèle de référence et utiliser dans des algorithmes pour vérifier l'identité de l'apprenant.

Le système doit être **adapté au contexte des formations en ligne**, c'est-à-dire qu'il doit prendre en compte des valeurs et des mesures générées par la plate-forme d'apprentissage (note d'un examen ou d'un qcm, taux de partici-

1. Ce travail a été réalisé dans le cadre du projet OFS - Open Food System, programme investissements d'avenir

2. `http://ignition-factory.com/fr/`

pation au forum, durée de suivre une session, etc.) pour authentifier les apprenants.
Le système que nous décrivons dans cet article, repose d'une part sur la combinaison intelligente de mécanismes d'authentification existants, et d'autre part sur un module d'authentification à partir de traces d'interaction. Les différentes sources d'authentification disponibles sont combinées et pondérées de sorte à déterminer un taux de certitude associé à l'authentification établie.
Les problématiques scientifiques liées à la création de ce système, sont diverses et de complexité croissante : identifier les moyens d'authentification disponibles chez les apprenants ; savoir comment combiner les différentes informations d'authentification ; savoir à quel moment déclencher une alerte et vérifier l'identité de l'utilisateur effectuant l'activité pour confirmer ou infirmer son identité ; définir des mesures de confiance et des métriques pour garantir l'identité d'un utilisateur connecté ; être capable de s'adapter au contexte de l'activité ; et enfin, construire un mécanisme d'authentification à partir des traces d'interaction d'un utilisateur avec un environnement informatique.
Dans la section suivante, après un rappel du contexte et des contraintes qui lui sont liées, nous présentons un état de l'art des méthodes d'authentification existantes. Ensuite, dans la section 3, nous présentons l'architecture générale du système que nous proposons, ainsi que les composants qui ont déjà été réalisés. Enfin, en section 4, nous discutons des questions de recherche que nous avons identifiées. Nous mettons en particulier l'accent sur la problématique de l'authentification à partir des traces d'interaction qui est le principal enjeu scientifique de cette thèse.
L'ensemble de ce travail est réalisé dans le cadre d'une thèse qui vient de débuter, en collaboration entre le LIRIS et la société Ignition Factory.

2 Contexte et état des lieux quant à l'authentification

Nos travaux s'inscrivent dans le cadre du développement d'une nouvelle plate-forme de formation en ligne (LMS, Learning Management System) à destination des entreprises (TPE/PME) et des professionnels indépendants. Cette plate-forme développée par la société Ignition Factory vise à combler certains points faibles de la formation en ligne, à savoir le contrle de l'identité et des connaissances, ainsi que les lourdeurs administratives pour la formation professionnelle. Ignition Factory propose pour cela deux axes d'innovation principaux : le premier vise à automatiser les démarches administratives et à faciliter l'accès aux formations et à leur remboursement ; le deuxième cherche à résoudre le problème de l'authentification des utilisateurs afin de délivrer les certifications, avec comme objectif idéal de donner une garantie de l'identité des utilisateurs équivalente à celle des formations traditionnelles en présence. C'est ce second axe qui nous concerne tout particulièrement et que nous allons développer dans la suite de l'article. Nous présentons dans la suite une étude des différentes méthodes d'authentification des utilisateurs, dans un contexte général, puis dans le contexte spécifique de l'apprentissage en ligne.

2.1 Approches classiques de l'authentification

L'authentification est le processus de vérification de l'identité des utilisateurs. La littérature [1] organise les approches d'authentification des utilisateurs en trois catégories : authentification à base de connaissances (i.e. en fonction de questions / réponses), authentification à base d'objets et authentification biométrique.
L'authentification à base de connaissances est la méthode qui permet de vérifier l'identité des utilisateurs en se basant sur des informations mémorisées par le système lors de la phase d'inscription, par exemple un mot de passe ou une réponse à une question de sécurité. Ce sont les méthode d'authentification les plus populaires et classiques puisque les données d'authentifications sont faciles à mémoriser par les utilisateurs. En raison de la facilité à contourner ce type de système lorsque l'utilisateur a la volonté de partager ses identifiants, nous ne réaliserons pas une analyse détaillée des différentes approches.
L'authentification à base d'objets est une approche selon laquelle les utilisateurs sont authentifiés par les informations contenues dans un objet physique en leur possession, par exemple une clé USB ou une carte électronique. Dans les examens en ligne, la présence d'un tel objet pour vérifier l'identité des utilisateurs peut augmenter le degré de sécurité des informations, mais ces objets peuvent également être perdus ou prêtés, ce qui nous ramène au problème précédent. De plus, de telles méthodes ajoutent de fortes contraintes matérielles (nécessité d'avoir des lecteurs de cartes par exemple).
L'authentification biométrique est l'ensemble des techniques et méthodes qui permettent la vérification automatique de l'identité des personnes sur la base des caractéristiques physiologiques et/ou comportementales [2]. Nous allons maintenant détailler les méthodes d'authentification biométriques. Ces méthodes peuvent être classées en deux catégories : les méthodes basées sur l'analyse des traits physiques qui sont particuliers, distincts et permanents pour chacun, tel que les empreintes digitales, la forme de la main, le fond de l'oeil, etc. ; et les autres méthodes fondées sur l'analyse du comportement et des actions de l'utilisateur tels que l'analyse de la signature, la dynamique de frappe clavier et la façon d'utiliser la souris. Les approches d'authentification physiques permettent d'avoir un pourcentage élevé de certitude mais ils exigent en contrepartie la disponibilité d'appareils de mesure coteux et parfois peu répandus (caméra, capteur d'empreintes digitales, etc.) alors que les systèmes d'authentification comportementaux sont moins coteux puisque l'on peut capter les informations nécessaires au moyen de dispositifs courants (clavier et souris).
Parmi ces méthodes nous citons celles les plus répandues

et utilisées dans le contexte de la formation en ligne [3].

La reconnaissance des empreintes digitales : c'est une technique biométrique qui se base sur l'identification de l'utilisateur par ses empreintes digitales. Ces techniques d'authentification sont les plus utilisées et répandues dans les applications de sécurité, par exemple pour le contrôle d'accès. Différentes techniques permettent de capturer les images d'une empreinte digitale telle que les capteurs optiques, capteurs en silicium, capteurs ultra sonique, etc.

La reconnaissance faciale [4] : c'est la méthode de d'authentification des utilisateurs par les traits du visage. Le principal avantage de cette méthode est de ne pas être intrusive. De plus, les algorithmes appliqués dans ces méthodes d'authentification ont connu des progrès très importants ces dernières années. Les approches de reconnaissance du visage sont fondées sur des algorithmes qui permettent de mesurer des attributs faciaux comme la distance entre les yeux, la position du menton, etc.

La reconnaissance vocale : c'est une technique qui se base sur les caractéristiques de la parole, uniques chaque personne. Les techniques de la reconnaissance vocale se basent sur l'analyse des caractéristiques quantitatives, par exemple la fréquence, les harmoniques, la puissance sonore, etc.

La dynamique de frappe au clavier [5] : la dynamique de frappe est une modalité biométrique comportementale qui permet d'identifier les personnes en mesurant leur façon de taper au clavier. Plus précisément, la méthode génère un comportement de frappe comme modèle de référence (une signature). Ce modèle est obtenu par la combinaison des attributs tels que la durée d'une frappe, la vitesse de frappe, le temps de latence entre l'appui des touches, le temps entre le relâchement d'une touche et la pression d'une autre, le temps entre deux relâchements de touches, etc.

La dynamique du mouvement de la souris [6] : la dynamique du mouvement de la souris est une technologie de la biométrie comportementale récemment proposée [7] qui permet d'identifier les utilisateurs en se basant sur l'analyse des clics et des mouvements de la souris. Les évènements de la souris sont généralement insuffisants (clic double, clic simple, molette) pour l'analyse d'un comportement, mais des algorithmes de regroupement ont été proposés pour obtenir des informations de plus haut niveau (trajet d'un mouvement puis clic, glisser-déposer, etc.) à partir desquels des modèles de référence significatifs peuvent être détectés. Des études ont démontré que la dynamique de la souris a un fort potentiel en tant que méthode d'identification des utilisateurs [8].

Combinaison des méthodes biométriques : D'autres études ont analysé la question de combiner plusieurs méthodes biométriques afin de créer un système d'authentification plus performant appelé «système d'authentification multi-modèles» (Mutimodal Biometric System MBS) [9]. Toutes les études présentées par Sahoo et al. [9] sur les MBS montrent une amélioration des performances suite à cette combinaison d'informations issues de méthodes biométriques distinctes. Un MBS intégrante les méthodes d'authentification par empreintes digitales et par caractéristiques du visage et de la voix est implémenté dans [10]. Les résultats de cette expérience montrent que la combinaison de différentes méthodes d'authentification est efficace pour surmonter les limitations de l'implémentation d'une seule méthode. D'autres études, comme [11], ont proposé un système d'authentification continue qui est fondé sur l'analyse du comportement des utilisateurs. Les méthodes utilisées dans cette approche sont la dynamique de frappe et la dynamique de mouvement de la souris. Les résultats obtenus par cette recherche sont prometteurs mais ils ne sont pas encore suffisamment fiables pour être déployés en conditions réelles.

2.2 L'authentification dans les plates-formes d'apprentissage

De nombreuses études ont appliqué les différents méthodes d'authentification citées ci-dessus dans différents domaines de la formation en ligne, tel que les MOOCs, les examens en ligne et les systèmes d'apprentissage en ligne. Une solution d'authentification par les connaissances dans les formations en ligne a été proposée dans les travaux [[12], [13]] d'A. Ullah. Ces derniers proposent un système basé d'une part sur le profil de l'utilisateur (Profile Based Authentication Framework, PBAF) et d'autre part sur l'identifiant et le mot de passe. L'apprenant se connecte à la plate-forme par son identifiant et mot de passe, puis est invité à répondre à un ensemble de questions de sécurité durant la phase d'apprentissage afin de générer son profil. Lors de l'accès aux examens en ligne, il doit répondre correctement à une liste de questions sélectionnées aléatoirement.

L'authentification biométrique est la plus répandue dans le domaine de la formation en ligne. En effet, plusieurs recherches ont été effectuées récemment pour l'application d'une ou d'un ensemble des méthodes d'authentification biométriques citées ci-dessus au sein des plates-formes de formation en ligne.

Des études comme [14], [15] ont proposé une intégration de la méthode d'authentification par la reconnaissance des empreintes digitales dans les plates-formes d'apprentissage, y compris dans la plate-forme de formation en ligne MOODLE [15]. Ce dernier (Fingerprint Identification System) implique un traitement d'image et d'extraction des informations à partir de l'image de l'empreinte digitale.Il est vrai que ce système permet de garantir la présence de l'apprenant au moment de l'identification, mais au prix d'un scanner d'empreintes digitales.

D'autres recherches [16], [17] ont proposé l'implémentation d'un système de reconnaissance faciale dans les plates-formes d'apprentissages. L'authentification faciale est généralement une méthode fiable pour l'identification, mais la variation des qualités des webcams en plus des conditions d'éclairage chez les apprenants ne permettent pas toujours d'avoir une image d'une qualité suffisante pour les

authentifier.
D'autres études se basent sur le comportement des apprenants via les frappes clavier pour avoir une authentification continue dans les examens en ligne [18]. L'utilisation de l'analyse de frappe clavier pour caractériser un comportement de l'utilisateur parane méthode intéressante, mais ne peut pas être le seul critère. En effet, sur certaines activités l'utilisateur n'utilise pas le clavier.
L'authentification par une seule méthode étant facilement sujette à échecs, certains travaux ont donc opté pour des MBS dans les formations en ligne. Dans [19], le système est basé sur l'authentification via les empreintes digitales et sur les mouvements de souris. La dynamique des mouvements de souris est utilisée pour gérer le comportement de l'utilisateur et la reconnaissance des empreintes permet d'augmenter la sécurité de l'authentification.
Dans le contexte des MOOCs, actuellement, seule la plateforme Coursera applique l'authentification biométrique pour la certification des apprenants [20] via son système nommé « signature Track » [21]. Ce système est basé sur deux approches d'authentification biométriques : la reconnaissance faciale et la reconnaissance du rythme de frappe clavier. Lors de l'inscription, le système demande de prendre une photo via une webcam, de fournir un scan de la carte d'identité et enfin de saisir une courte phrase. Une vérification de l'image de la webcam et de la photo des pièces d'identité est effectuée par Coursera, ensuite le scan de La pièce d'identité est supprimée. Pendant le suivi du cours, et à chaque évaluation (test, quiz, etc.) la plateforme demande de faire la même chose (photo webcam et saisir une phrase). La combinaison de ces deux caractéristiques biométriques constitue le processus de vérification de l'identité.

2.3 Synthèse et discussion

Nous avons présenté les principales méthodes d'authentification, et en particulier les approches biométriques, indépendamment de leur contexte d'application, puis nous avons présenté une sélection de systèmes d'authentifications spécifiquement liés aux environnements de la formation en ligne. Nous vérifions dans cette partie si ces systèmes répondent aux contraintes que nous avons identifiées et que nous reprenons ici et résumons dans le tableau 1 :
-**Être indépendant du contexte matériel (ICM)** de l'apprenant : en fait on cherche une solution non invasive (n'oblige pas les apprenants pour être filmé, photographié ou parlé) et destiné à toute personne équipée d'un ordinateur d'autent plus que l'on s'adresse au public professionnel.
-**Permettre une authentification continue (AC)** en authentifiant l'utilisateur tout au long de la formation, et pas uniquement au début ou à sa clôture.
-**Avoir une signature de l'utilisateur dynamique (D)** qui permet de prendre en compte le changement de comportement des apprenants au cours du temps.
-Permettre la **combinaison de différentes solutions d'authentification** (CSA).
-**Avoir un composant comportemental** (C) : Cette piste mérite d'être explorer puisqu'elle répond à certain limitations des approches existants.
-**S'intégrer au contexte de la formation en ligne** (CFL), ce qui signifie que le système doit s'adapter aux différentes activités pédagogiques (contenue du rédactionnel, vidéos, quiz, etc.).

TABLE 1 – Validation des contraintes par les travaux existants

Approche	ICM	CFL	AC	D	CSA	C
PBAF [12]	x		x	x		
FIS [15]						
Face recognition [17]						
Keystroke [18]	x		x			x
Multimodal [19]					x	x
Signature Track [21]					x	x

Nous constatons qu'aucune des méthodes proposées ne répond à tous nos critères. Dans le cas de l'adaptation au contexte de la formation en ligne, nous n'avons trouvé aucune méthode qui remplisse ce critère. Une première piste est de combiner ces approches. En supposant que cela soit possible, la combinaison de PBAF et Signature Track validerait cinq des six critères que nous avons fixés, ce qui permettrait de couvrir un bien plus large panel de situations, et renforcerait peut-être la certitude accordée à l'authentification finale. Néanmoins, le critère de l'adaptation au contexte de la formation en ligne, pourtant critique à notre avis, n'est toujours pas traité. Il nous faut donc explorer une nouvelle approche, jamais abordée dans ce contexte à notre connaissance.

3 Une approche d'authentification à base de traces

Le système d'authentification que nous proposons dans cet article repose sur une nouvelle approche : l'authentification des utilisateurs à partir de leurs traces d'interaction. Une trace d'interaction est un enregistrement de l'ensemble des actions effectuées par l'utilisateur dans un système. Ces traces sont un bon moyen pour capturer les activités des apprenants dans les plates-formes de formation en ligne sous la forme des inscriptions numériques d'une manière homogène, difficilement falsifiable et indépendant du contexte dans lequel l'utilisateur se situe. De plus on peut obtenir ces informations sans avoir de dispositif supplémentaire. Cependant, pour que ces traces capturées soient réutilisables et exploitables au sein d'un processus d'authentification, il faut s'appliquer à choisir la manière de les représenter et de les collecter. En effet, pour que ces traces d'interaction puissent devenir une source de connaissance pour l'identification des utilisateurs, elles doivent être correctement formalisées et nous devons disposer d'outils pour les exploiter. Pour cela, nous nous appuyons sur une représen-

tation de l'activité d'apprentissage sous forme des traces modélisées.
Le concept des traces modélisées (M-Trace) a été proposé par l'équipe SILEX du LIRIS [22]. Une trace modélisée est un objet informatique qui permet de décrire d'une manière détaillée les actions effectuées par les utilisateurs sur un système d'information pendant une durée déterminée. Une trace modélisée est toujours associée à un modèle contenant la définition des types des éléments qui la composent ainsi que leurs relations. Nous avons déjà une bonne expérience en matière d'exploitation des traces modélisées, et en particulier dans le contexte des plates-formes d'enseignement. En effet, nous avons proposé une architecture pour observer des activités d'apprentissage et les collecter sous forme des traces modélisées [23]. Un assistant Samo-TraceMe [3] a été conçu pour fournir des outils d'exploitation de ces traces collectées. Nous souhaitons nous appuyer sur notre expérience et étendre les outils que nous avons développés pour traiter la problématique de l'authentification.
Une architecture d'authentification par les traces modélisées est représentée dans la figure 1. L'acheminement des traces passe par les trois composants principaux :
-Le premier c'est l'outil responsable de la collecte de l'activité d'apprentissage. Le processus de collecte que nous proposons se divise en deux phases : la phase de spécification du traçage au cours de laquelle les concepteurs de la formation spécifient les événements qu'il souhaitent collecter sur des éléments identifiés par leur sélecteurs. La deuxième phase est la phase d'exécution de la collecte. Cette phase est inspirée du système de collecte TraceMe [4] [23] qui permet le traçage d'une activité d'apprentissage dans les MOOCs en prenant en compte les actions provenant du coté serveur de l'application et les interactions produites par le navigateur côté client. La limitation de ce système est que la collecte côté client doit se faire par l'installation volontaire par les utilisateurs d'une extension pour les navigateurs. Il existe donc un risque plus important de perdre les traces côté client si l'utilisateur choisit de ne pas l'installer, ou qu'il oublie de l'activer. Nous envisageons donc plutôt un script persistant qui s'intègre dans les pages webs de la plate-forme afin de collecter directement les traces de navigation de l'utilisateur selon une configuration définie dans la phase précédente.
-Le deuxième composant permet le stockage des traces collectées. Nous nous appuyons dans ces travaux sur le système KTBS [5] (Kernel Trace Base System). Il s'agit d'un logiciel open source qui permet de stocker des traces et leur modèle et permet également de calculer des traces transformées à l'aide d'un ensemble d'opérateurs (filtre, fusion, requête-Sparql). Le KTBS est développé comme un service web RESTful qui permet une communication via le protocole HTTP avec n'importe quelle application (quel que soit le langage de programmation et le système d'exploitation). Il utilise la représentation RDF pour le stockage des données afin de pouvoir capturer la sémantique de ces informations. Il permet aussi d'échanger ces données au format JSON.
-Le troisième est un ensemble de plusieurs modules qui permettent d'effectuer des transformations et des calculs de mesures sur les traces stockées. Ce composant représente le noyau de nos prochains travaux de recherches.

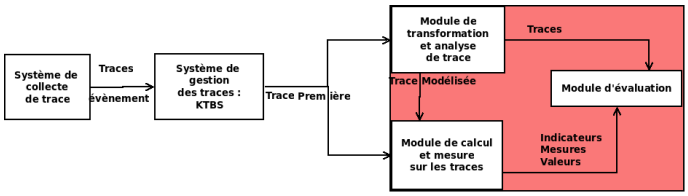

FIGURE 1 – Architecture du système d'authentification se de trace

4 Conclusion et questions de recherche

La problématique centrale de notre thèse est : est-il possible d'authentifier un utilisateur à partir de ses traces d'interaction ? Cette question majeure soulève d'autres problématiques et se confronte à des enjeux techniques significatifs. Nos premières réflexions nous ont amenés à identifier certains de ces éléments, que nous prévoyons d'approfondir dans le cadre de cette thèse.
Tout d'abord, se posent les questions éthiques. Dans quelle mesure une telle approche peut-elle être mise en place ? Présente-t-elle des risques ? Sera-t-elle acceptée par les utilisateurs dans le contexte de l'obtention de certificats dans un milieu professionnel ? Quelles garanties doit-on offrir, notamment en matière de sécurité et de visibilité des données collectées ? Comment bâtir une solution efficace tout en respectant la vie privée et le droit d'accès aux données des utilisateurs ?
Ensuite, se posent les questions liées à la démarche que nous souhaitons employer pour ce premier volet de notre travail. En effet, nous souhaitons mettre en place une approche inspirée d'autres méthodes d'authentification comportementales, et nous nous posons donc des questions similaires. Existe-t-il des éléments et des invariants dans les traces qui permettent d'identifier des utilisateurs ? Si oui comment peut-on les définir et les identifier ? Qu'en est-il de la fiabilité de l'approche ? Comment peut-on mesurer le degré de certitude et évaluer l'efficacité de nos mesures ? Comment utiliser ces valeurs dans un contexte pratique ?
Notre travail contient également un second volet qui consiste à proposer un algorithme permettant la combinaison intelligente de méthodes d'authentification selon leur disponibilité. Pour cela, il nous faudra être capable de ré-

3. https://github.com/fderbel/Assistant-Samo-Trace-Me
4. https://github.com/fderbel/Trace-Me
5. https://kernel-for-trace-based-systems.readthedocs.org/en/latest/

pertorier et caractériser les différentes méthodes d'authentification, de vérifier si elles sont disponibles chez les apprenants et de les solliciter au bon moment. Ensuite, il nous faudra proposer un modèle permettant de les combiner et de les pondérer en fonction de la confiance que l'on pourra leur accorder. L'ensemble de ces travaux fera l'objet d'une implémentation dans la plate-forme d'enseignement développée par la société Ignition Factory. Cette plate-forme nous permettra de tester nos outils et de mettre à l'épreuve notre hypothèse principale.

Références

[1] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," vol. 91, no. 12, pp. 2021–2040.

[2] Z. Riha *et al.*, "Toward reliable user authentication through biometrics," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 45–49, 2003.

[3] K. Delac and M. Grgic, "A survey of biometric recognition methods," in *Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium*. IEEE, 2004, pp. 184–193.

[4] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition : A literature survey," *Acm Computing Surveys (CSUR)*, vol. 35, no. 4, pp. 399–458, 2003.

[5] P. S. Teh, A. B. J. Teoh, and S. Yue, "A survey of keystroke dynamics biometrics," *The Scientific World Journal*, vol. 2013, 2013.

[6] Z. Jorgensen and T. Yu, "On mouse dynamics as a behavioral biometric for authentication," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. ACM, 2011, pp. 476–482.

[7] A. A. E. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," *Dependable and Secure Computing, IEEE Transactions on*, vol. 4, no. 3, pp. 165–179, 2007.

[8] C. Shen, Z. Cai, X. Guan, Y. Du, and R. A. Maxion, "User authentication through mouse dynamics," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 1, pp. 16–30, 2013.

[9] S. K. Sahoo, T. Choubisa, and S. M. Prasanna, "Multimodal biometric person authentication : A review," *IETE Technical Review*, vol. 29, no. 1, pp. 54–75, 2012.

[10] A. K. Jain, L. Hong, and Y. Kulkarni, "A multimodal biometric system using fingerprint, face and speech," in *Proceedings of 2nd Int'l Conference on Audio-and Video-based Biometric Person Authentication, Washington DC*, 1999, pp. 182–187.

[11] S. Mondal and P. Bours, "Continuous authentication in a real world settings," in *Advances in Pattern Recognition (ICAPR), 2015 Eighth International Conference on*. IEEE, 2015, pp. 1–6.

[12] A. Ullah, H. Xiao, and M. Lilley, "Profile based student authentication in online examination," in *Information Society (i-Society), 2012 International Conference on*. IEEE, 2012, pp. 109–113.

[13] A. Ullah, H. Xiao, T. Barker, and M. Lilley, "Evaluating security and usability of profile based challenge questions authentication in online examinations," *Journal of Internet Services and Applications*, vol. 5, no. 1, p. 2, 2014.

[14] C. Gil, M. Castro, and M. Wyne, "Identification in web evaluation in learning management system by fingerprint identification system," in *Frontiers in Education Conference (FIE)*, 2010.

[15] S. Alotaibi, "Using biometrics authentication via fingerprint recognition in e-exams in e-learning environment," 2010.

[16] E. G. Agulla, L. A. Rifón, J. L. A. Castro, and C. G. Mateo, "Is my student at the other side ? applying biometric web authentication to e-learning environments," in *Advanced Learning Technologies, 2008. ICALT'08. Eighth IEEE International Conference on*. IEEE, 2008, pp. 551–553.

[17] Q. Zhao and M. Ye, "The application and implementation of face recognition in authentication system for distance education," in *Networking and Digital Society (ICNDS), 2010 2nd International Conference on*, vol. 1. IEEE, 2010, pp. 487–489.

[18] E. Flior and K. Kowalski, "Continuous biometric user authentication in online examinations," in *Information Technology : New Generations (ITNG), 2010 Seventh International Conference on*. IEEE, 2010, pp. 488–492.

[19] S. Asha and C. Chellappan, "Authentication of e-learners using multimodal biometric technology," in *Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on*. IEEE, 2008, pp. 1–6.

[20] P. Bond, "Biometric authentication in moocs," 2013.

[21] A. Maas, C. Heather, C. T. Do, R. Brandman, D. Koller, and A. Ng, "Offering verified credentials in massive open online courses : Moocs and technology to advance learning and learning research (ubiquity symposium)," *Ubiquity*, vol. 2014, no. May, p. 2, 2014.

[22] P.-A. Champin, A. Mille, and Y. Prié, "Vers des traces numériques comme objets informatiques de premier niveau : une approche par les traces modélisées," *Intellectica*, vol. 59, pp. 171–204, 2013.

[23] A. Cordier, F. Derbel, and A. Mille, "Observing a web based learning activity : a knowledge oriented approach," Ph.D. dissertation, LIRIS UMR CNRS 5205, 2015.