UQAC
Université du Québec
à Chicoutimi

SYSTÈME D'AUTHENTIFICATION À DEUX FACTEURS ZERRO-EFFORT ET CONTINU EXPLOITANT LES SIGNAUX AUDIO AMBIANTS ET LES SIGNAUX BLUETOOTH LOW ENERGY (BLE) POUR LA DETECTION DE COLOCALISATION

PAR BAKAYOKO ISSOUF

MÉMOIRE PRÉSENTÉ À L'UNIVERSITÉ DU QUÉBEC À CHICOUTIMI EN VUE DE L'OBTENTION DU GRADE DE MAÎTRE ÈS SCIENCES (M. SC.) EN INFORMATIQUE

QUÉBEC, CANADA

RÉSUMÉ

L'authentification à deux facteurs (2FA) renforce considérablement la sécurité par rapport aux schémas traditionnels basés sur le couple nom d'utilisateur–mot de passe. Cependant, les mécanismes 2FA classiques, tels que les codes à usage unique (OTP) envoyés par SMS, imposent souvent des contraintes d'utilisabilité et perturbent l'expérience utilisateur. Pour pallier ces limitations, nous proposons SBLE, une nouvelle approche 2FA sans interaction et continue, qui vérifie l'identité de l'utilisateur de manière transparente. SBLE combine les signaux audio ambiants et les signaux Bluetooth Low Energy (BLE), notamment les adresses MAC et les valeurs RSSI, afin d'authentifier les utilisateurs de manière robuste. Lors d'une tentative de connexion, l'ordinateur de l'utilisateur et un smartphone de confiance à proximité enregistrent simultanément les caractéristiques de leur environnement, incluant les signaux BLE et le son ambiant. L'application SBLE sur le smartphone analyse la similarité entre les deux enregistrements pour déterminer si les appareils sont physiquement colocalisés, puis prend la décision d'authentification en conséquence. Le système repose sur le principe selon lequel seuls deux appareils situés à proximité partagent des caractéristiques environnementales similaires, permettant ainsi de distinguer les utilisateurs légitimes des adversaires, même en situation de coprésence. Les expériences menées en conditions réelles montrent que SBLE surpasse les systèmes existants en termes de résilience face aux attaquants distants et coprésents, tout en maintenant une expérience utilisateur fluide. Le système atteint une précision de 94,04% et un taux de fausse acceptation de 3,22%, même dans des environnements adverses complexes. SBLE représente ainsi une solution pratique, sécurisée et transparente pour une authentification mobile robuste, continue et conviviale.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS

2FA Two Factor Authentification
BLE Bluetooth Low Energy
RSSI Received Signal Strength Indicator
BD-ADDR Bluetooth Adress
AES Advanced Encryption Standard
RSA Rivest Shamir Adleman (public-key cryptography algorithm)
TLS Transport Layer Security
NFC Near Field Communication
MiTM Man-in-the-middle
DoS Denial of Service
API Application Programming Interface
HTML HyperText Markup Language
FAR False Acceptance Rate
FRR False Rejection Rate

DÉDICACE

À mon père et à ma mère.

Je vous dédie ce travail en espérant que vous serez toujours fiers de moi.

Je dédie également ce travail à tous les membres de la famille, pour leurs encouragements, soutiens, affectation et confiance pour continuer mes études.

Au Professeur Fehmi Jaafar qui m'a donné confiance et espoir et qui m'a soutenu durant toutes mes recherches.

À tous ceux qui de près ou de loin ont contribué de quelques manières à la réalisation de ce document.

Qu'ALLAH leur accorde la santé, prospérité et leur gratifie de sa miséricorde.

REMERCIEMENTS

Je remercie, en premier lieu, ALLAH pour le courage, la patience et la santé qu'il m'a donné pour poursuivre mes études.

Je tiens à exprimer ma sincère reconnaissance à mon directeur de recherche, professeur Fehmi Jaafar, pour son soutien constant et précieux. Son expertise, ses conseils avisés et sa disponibilité ont été des atouts majeurs dans la réalisation de ce projet. Je lui suis particulièrement reconnaissant pour les bourses d'études qu'il m'a attribuées, lesquelles ont grandement facilité le bon déroulement de mes recherches. Sa capacité à m'inspirer et à me challenger intellectuellement m'a permis de repousser mes limites.

Je souhaite également exprimer ma reconnaissance envers tous les professeurs que j'ai eus la chance de croiser tout au long de mon parcours académique. Leurs enseignements, riches et éclairants, ont joué un rôle clé dans la construction de mes connaissances et compétences. Plus particulièrement, je tiens à remercier Monsieur Mohamed Tahar Bennani et Monsieur Pascal Fortin, dont les enseignements et orientations ont grandement contribué à mon développement académique.

Mes remerciements s'adressent aussi à l'ensemble du personnel du département de mathématiques et informatique (DIM) de l'UQAC.

Enfin, merci à ma famille, mes amis et mes proches pour m'avoir toujours aidé à trouver un équilibre entre les études et vie personnelle.

AVANT-PROPOS

Ce mémoire de maîtrise marque l'aboutissement d'un parcours académique à la fois exigeant et profondément enrichissant, au cours duquel j'ai eu l'occasion d'explorer des domaines passionnants tels que la cybersécurité, l'intelligence artificielle, les systèmes intelligents et l'Internet des objets (IoT). Grâce aux cours, aux stages et aux recherches menées en laboratoire, j'ai pu acquérir de solides compétences dans des domaines variés, notamment le développement d'applications, l'apprentissage automatique, et plus particulièrement la cybersécurité. J'ai également eu l'opportunité d'approfondir l'étude des systèmes d'authentification à deux facteurs et d'authentification continue, en analysant leur rôle essentiel dans la protection des identités numériques.

L'objectif de ce travail est de démontrer comment l'exploitation de données environnementales, telles que le son ambiant et les signaux Bluetooth Low Energy (BLE), peut contribuer à renforcer la fiabilité de l'authentification à deux facteurs et continue. Cette approche vise non seulement à améliorer la détection des attaques, mais également à offrir une expérience utilisateur fluide et sans effort, dans un contexte où la vérification d'identité demeure primordiale.

Ce parcours de recherche a été jalonné de défis, de périodes de doute, de stress et de moments de persévérance, mais aussi de découvertes marquantes et de réalisations gratifiantes. Chaque page de ce mémoire reflète les nombreuses heures consacrées à la recherche, à la réflexion et à l'analyse, dans le but constant d'approfondir la compréhension du sujet.

Je prends l'entière responsabilité des propos tenus dans ce document. Cependant, conscient que toute œuvre humaine peut être améliorée, je vous serai reconnaissant de toute remarque, critique ou suggestion visant à enrichir cette étude. C'est dans cette optique, que ce travail a été soumis pour évaluation à la conference ACM, The 16th ACM Conference on Data and Application Security and Privacy (CODASPY), en vue d'une éventuelle publication.

Puissent les résultats de ce mémoire non seulement valider mon parcours académique, mais aussi ouvrir de nouvelles perspectives de recherche pour contribuer à un avenir numérique plus sûr. C'est avec humilité et un profond sentiment de contribution, aussi modeste soit-elle, que je vous invite à découvrir ce travail.

CHAPITRE I

INTRODUCTION

1.1 CONTEXTE DE RECHERCHE

À mesure que la technologie continue d'évoluer à un rythme rapide, la nécessité de mécanismes de sécurité robustes pour protéger les informations et les données sensibles devient primordiale. Selon le Identity Theft Resource Center (ITRC), les violations de données ont augmenté de plus de 68% en 2020, avec un total de 1 862 incidents signalés AlQahtani *et al.* (2024). En réponse à ces menaces, l'adoption de l'authentification à deux facteurs (2FA) a connu une croissance significative. Une étude réalisée par Google en 2020 a révélé que plus de 150 millions d'utilisateurs s'appuient désormais sur la 2FA pour sécuriser leurs comptes, un chiffre appelé à croître à mesure que la cybersécurité devient une priorité pour les particuliers et les organisations Cipriani (2022). Par ailleurs, des recherches menées par Microsoft ont démontré que la 2FA peut contrecarrer 99,9% des cyberattaques automatisées Maynes (2019). Ainsi, la 2FA est devenue un outil essentiel pour sécuriser l'accès aux systèmes sensibles. Cette tendance est confirmée par une étude du Ponemon Institute, selon laquelle 56% des organisations américaines ont mis en œuvre une forme de 2FA pour au moins une partie de leur personnel Jayson (2020).

1.2 AUTHENTIFICATION À DEUX FACTEURS

L'authentification à deux facteurs renforce l'authentification traditionnelle en exigeant un facteur supplémentaire au-delà du simple mot de passe. La nature de ce second facteur a été largement explorée dans la littérature, notamment dans les travaux de Oren & Arad (2022), Hong *et al.* (2021) et He *et al.* (2022), où les chercheurs ont examiné différents

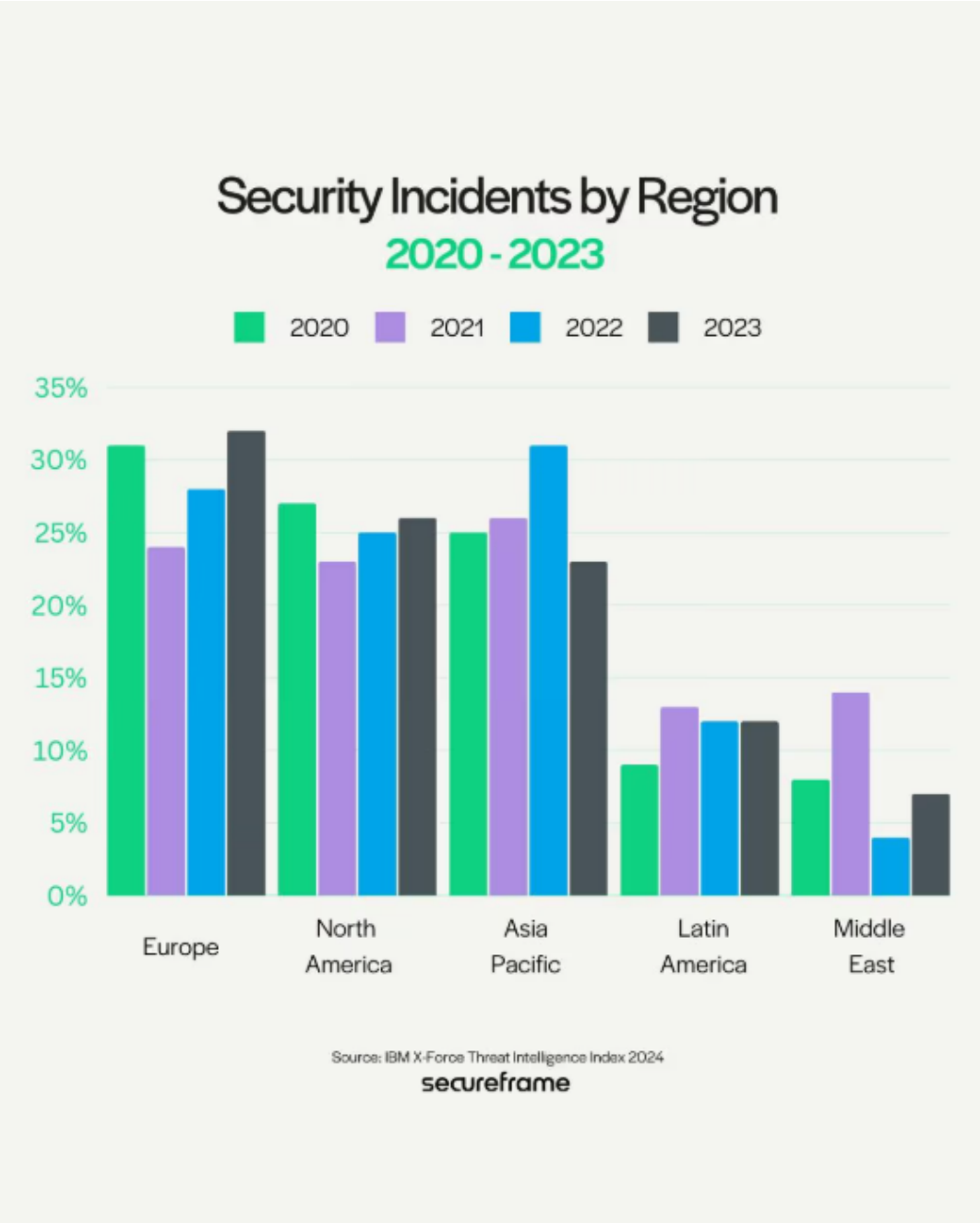


FIGURE 1.1 : Incidents de sécurité de 2020 - 2024 dans le monde.

(Bonnie, 2025)

types de facteurs : basés sur la connaissance, la possession, la biométrie, la localisation, le comportement ou encore le contexte environnemental AlQahtani *et al.* (2021). Chacun de

ces facteurs vise à vérifier de manière unique l'identité de l'utilisateur tout en renforçant la sécurité globale de l'information. Cependant, dans la pratique, de nombreux utilisateurs continuent de privilégier l'authentification par nom d'utilisateur et mot de passe lorsque la 2FA est optionnelle Petsas *et al.* (2015). L'une des principales raisons est que les mécanismes 2FA traditionnels imposent souvent une charge supplémentaire à l'utilisateur, telle que la saisie d'un code à usage unique reçu par SMS.

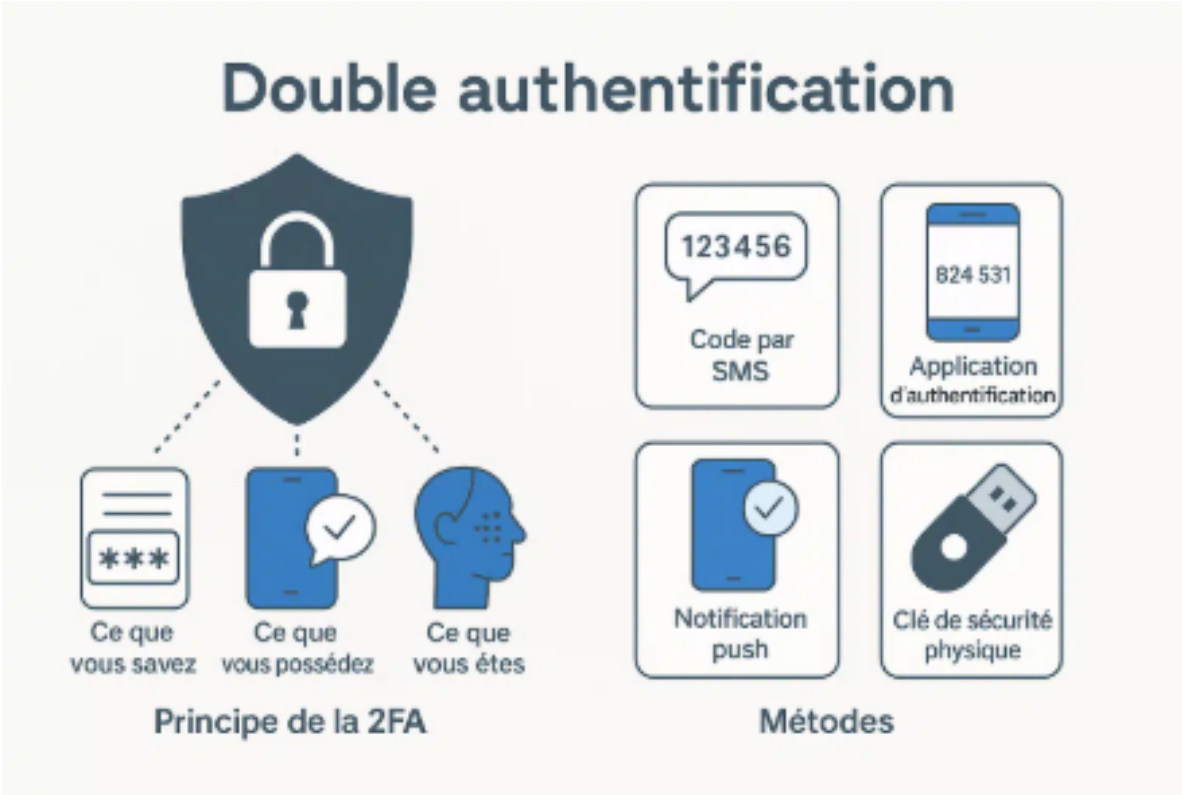


FIGURE 1.2 : Authentification à double facteurs

(Deloffre, 2025)

1.3 AUTHENTIFICATION À DEUX FACTEURS ZÉRO-EFFORT

C'est dans ce contexte que les systèmes 2FA dits zéro-effort ont vu le jour, dans lesquels le second facteur d'authentification ne nécessite aucune interaction supplémentaire de la part de l'utilisateur, celui-ci se contente juste d'entrer ses identifiants. On considère un scénario typique où un utilisateur tente de se connecter à un service Web via un navigateur de bureau, tandis qu'un smartphone à proximité facilite silencieusement l'authentification. Après l'enregistrement du téléphone en tant que jeton de sécurité, la connexion n'est autorisée que si le système peut confirmer que le téléphone est physiquement proche, selon le principe selon lequel un individu « ne peut pas être à deux endroits en même temps » Agadakos *et al.* (2016). Ainsi, la 2FA zéro-effort devient un problème de détection de co-localisation entre l'ordinateur et le smartphone de l'utilisateur, avec une implication minimale, voire nulle, de celui-ci.

Plusieurs travaux récents ont tenté de relever ce défi. Par exemple, le système ABLE Acar *et al.* (2020) exploite les signaux BLE environnementaux pour détecter la co-localisation. Il ne nécessite aucune interaction utilisateur et offre une bonne efficacité dans les environnements intérieurs riches en signaux BLE. Un exemple notable est Sound-Proof Karapanos *et al.* (2015), qui compare les sons ambiants enregistrés par les microphones des deux appareils pour détecter leur proximité. De plus, les travaux de AlQahtani *et al.* (2024) exploitent les signaux Wi-Fi et l'apprentissage automatique pour valider en continu la présence d'un utilisateur à partir de caractéristiques comportementales et environnementales. Cependant, cette approche nécessite que les deux appareils soient connectés au même réseau Wi-Fi, ce qui limite son applicabilité dans des contextes mobiles ou publics.

1.4 PROBLÉMATIQUE DE LA RECHERCHE

Les systèmes 2FA sans interaction ont été conçus pour offrir un compromis entre sécurité et facilité d'utilisation. Parmi eux, Sound-Proof Karapanos *et al.* (2015) et ABLE Acar *et al.* (2020) se distinguent comme des approches pionnières exploitant respectivement les signaux audio ambiants et BLE pour vérifier la co-localisation entre les appareils d'un utilisateur. Cependant, malgré leurs performances prometteuses, ces systèmes présentent des limitations majeures dans des environnements réels et dynamiques.

D'une part, Sound-Proof demeure vulnérable aux attaques de prédiction sonore Shrestha *et al.* (2016), dans lesquelles un attaquant distant peut simuler ou rejouer un environnement acoustique similaire afin de tromper le mécanisme de vérification. De plus, son fonctionnement exclusif sur la modalité audio le rend instable dans les environnements silencieux, ou lorsque le microphone d'un appareil est obstrué. D'autre part, ABLE, bien qu'exempt d'audio, souffre d'une forte dépendance au contexte BLE : il devient instable dans les zones dépourvues de signaux détectables ou saturées de dispositifs Bluetooth. Ces constats soulignent une lacune fondamentale : aucune des solutions existantes ne parvient à maintenir un niveau de sécurité et de fiabilité constant dans l'ensemble des environnements possibles (silencieux, bruyants, denses ou isolés).

La question centrale de cette recherche est donc : Comment concevoir une solution d'authentification hybride exploitant simultanément les caractéristiques des signaux BLE et des sons ambiants pour renforcer la sécurité, la robustesse et la continuité de l'authentification sans effort ?

L'hypothèse de recherche sous-jacente est que la fusion multi-modale des signaux BLE et audio, combinée à une architecture respectueuse de la vie privée, permettrait de réduire le

taux de fausses acceptations (FAR) et de faux rejets (FRR) tout en offrant une authentification continue, transparente et sécurisée.

1.5 CONTRIBUTION DE LA RECHERCHE

Cette recherche a pour objectif d'apporter plusieurs contributions au domaine de l'authentification à deux facteurs zero-effort. Plus précisément :

- Nous développons SBLE, un nouveau mécanisme 2FA sans effort, reposant sur la détection de colocalisation entre le smartphone de l'utilisateur et le poste de connexion. Contrairement aux approches existantes, SBLE combine simultanément les signaux audio ambiants et les signaux BLE pour renforcer la fiabilité de la vérification. Le système extrait et compare trois dimensions de similarité : les adresses MAC BLE détectées, la RSSI, et les composantes spectrales des sons ambiants, afin de déterminer si les deux dispositifs partagent effectivement le même environnement physique.
- Intégration de l'authentification continue : SBLE va au-delà de la simple vérification ponctuelle et prend en charge l'authentification continue en réévaluant périodiquement la co-localisation des appareils. Cela permet de protéger contre les accès non autorisés si l'utilisateur légitime s'éloigne de son poste.
- Nous avons implémenté un prototype comprenant un serveur d'authentification basé sur Flask (accessible via un navigateur web) et une application mobile Android. Nous évaluons SBLE dans trois environnements en tenant contre de deux positions (téléphone posé sur un bureau vs. dans une poche) et démontrons une performance robuste. Comparé à Sound-Proof, SBLE a atteint des taux de fausses acceptations significativement plus faibles tout en maintenant un taux de faux rejets comparable.
- Résilience dans des environnements variés : SBLE se montre robuste aussi bien dans des environnements silencieux que dans des contextes perturbés par du bruit BLE. Il est

immunisé contre les attaques à distance, qui constituent une menace majeure pour les systèmes 2FA, et offre plus de 94% de précision même contre des adversaires colocalisés, surpassant ainsi de nombreux systèmes 2FA contextuels qui peinent à fonctionner dans des espaces physiques partagés.

1.6 MÉTHODOLOGIE DE LA RECHERCHE

La méthodologie adoptée pour la conception et l'évaluation du système SBLE repose sur une approche expérimentale et analytique inspirée des méthodologies employées dans les travaux Karapanos *et al.* (2015), et He *et al.* (2022), tout en y intégrant des mécanismes de sécurité et de confidentialité renforcés.

1.6.1 CONCEPTION DE L'ARCHITECTURE SBLE

Une architecture hybride a été élaborée, intégrant simultanément deux canaux contextuels :

- Le canal audio, exploité pour capturer et comparer les formes d'onde ambiantes perçues par le smartphone et le poste de travail.
- Le canal BLE, utilisé pour extraire des caractéristiques de proximité telles que les adresses MAC des balises environnantes et les valeurs RSSI.

Ces deux flux sont ensuite fusionnés à l'aide d'un mécanisme de décision multicritère basé sur des mesures de similarité normalisées (corrélation maximale croisée, indice de Jaccard). Le système détermine ainsi la co-localisation effective entre les deux dispositifs.

1.6.2 IMPLÉMENTATION ET INTÉGRATION DU PROTOTYPE

Un prototype complet de SBLE a été développé :

- Serveur web, qui sert d'interface utilisateur et propose une API Flask gère l'authentification et la communication entre les appareils.
- Une application Android qui sert de jeton logiciel, assure la capture et la transmission des signaux BLE et audio et calcule les scores de similarité.

Le poste de travail (navigateur web) et le smartphone échangent des données chiffrées afin de garantir la confidentialité et l'intégrité des informations transmises.

1.6.3 ÉVALUATION EXPÉRIMENTALE

Des campagnes de tests ont été menées dans plusieurs environnements représentatifs : un bureau silencieux, un espace public bruyant, un environnement mixte.

Chaque scénario a été testé selon deux positions du smartphone (posé sur la table ou placé dans la poche de l'utilisateur). Les performances ont été mesurées à l'aide d'une matrice de confusion (TP, FP, TN, FN) et d'indicateurs dérivés tels que le FAR, le FRR et la taux de précision globale (Accuracy). Les résultats ont ensuite été comparés quantitativement à ceux de Sound-Proof pour valider les gains de performance de SBLE.

1.6.4 ANALYSE ET DISCUSSION

Les données obtenues ont été interprétées pour évaluer la robustesse du système, son comportement dans des environnements adverses et la balance entre usabilité et sécurité. Cette analyse a permis d'identifier les perspectives d'amélioration futures, notamment en matière

d'optimisation énergétique, d'adaptation dynamique du seuil de décision, et de son intégration dans les systèmes de contrôle d'accès .

1.7 STRUCTURE DU DOCUMENT

Le reste de ce mémoire est organisé en cinq chapitres principaux, chacun abordant un aspect clé de la conception, de la mise en œuvre et de l'évaluation du système SBLE.

- **Chapitre 2 : Travaux Connexes.** Dans ce chapitre, une discussion approfondie sur les travaux existants en matière d'authentification à deux facteurs et de détection de coprésence est présentée, mettant en évidence les avancées récentes et les lacunes existantes.
- **Chapitre 3 : Modèles, hypothèses et Concepts fondamentaux.** Dans ce chapitre, nous détaillons les modèles et hypothèses sur lesquels repose SBLE. Il rappelle également les concepts techniques nécessaires à la compréhension de notre approche, tels que les métriques de similarité utilisées pour la détection de co-localisation, les mécanismes d'analyse de signaux audio ambiants et des signaux BLE, et principes du BLE.
- **Chapitre 4 : Architecture et implémentation de SBLE.** Ce chapitre décrit l'architecture globale du système SBLE, en détaillant les interactions entre ses composants. L'implémentation pratique est ensuite présentée. Il met également en avant les mécanismes de synchronisation temporelle et de chiffrement assurant la fiabilité et la confidentialité des échanges.
- **Chapitre 5 : Évaluation expérimentale et analyse des résultats.** Ce chapitre expose la méthodologie expérimentale mise en œuvre pour évaluer SBLE. Les campagnes de tests ont été réalisées dans différents environnements et selon plusieurs conditions d'usage. Les résultats sont analysés à partir de métriques telles que le FAR, le FRR et la précision,

puis comparés à ceux de Sound-Proof afin d'évaluer la performance et la robustesse de SBLE.

- **Chapitre 6 : Discussion et Limites.** Ce chapitre discute les résultats, ses limitations ainsi que certaines améliorations possibles.
- **Conclusion et Recherche Future.** Ce chapitre résume les principales contributions de ce travail. Il conclut l'étude par une brève discussion sur les orientations et les applications futures potentielles afin d'améliorer la sécurité et la performance de SBLE.

CHAPITRE II

TRAVAUX CONNEXES

L'expansion rapide de l'IoT a exposé une vaste surface d'attaque, nécessitant des mesures de sécurité avancées. Ce chapitre donne un aperçu des recherches antérieures dans le sujet. Nous discuterons des solutions existantes en matière d'authentification à deux facteurs et de détection de coprésence, tout en soulignant leurs avantages, leurs limites et les défis qui subsistent, servant ainsi de base à la conception de SBLE.

2.1 APPROCHES BASÉES SUR DES DONNÉES ENVIRONNEMENTALES ET LA DÉTECTION DE PROXIMITÉ

Divers mécanismes 2FA sans effort, conçus pour authentifier les utilisateurs sans nécessiter d'interaction supplémentaire, ont été proposés dans la littérature. Parmi les exemples notables, on retrouve Acar *et al.* (2020), Ghose *et al.* (2023), Shah & Kanhere (2017), et Zhao *et al.* (2021). He *et al.* (2022) exploite les caractéristiques des signaux BLE provenant de l'environnement pour détecter la co-localisation. Vibe Husa & Tourani (2021) propose une autre approche en utilisant la communication par vibrations pour une authentification implicite et transparente de l'utilisateur.

De même, plusieurs systèmes tels que Sound-Login, Sound-Proof Karapanos *et al.* (2015), SoundAuth Wang *et al.* (2018), et Listening Watch Shrestha & Saxena (2018) mettent en œuvre le second facteur via un canal audio. Dans Sound-Login Cifrasoft (2019), le dispositif secondaire joue un code audio à usage unique généré par le dispositif principal, utilisé ensuite comme second facteur. Toutefois, ce protocole est vulnérable aux attaques de type MiTM, où un adversaire enregistre le son près du dispositif secondaire et le rejoue près du dispositif principal,

même si les deux sont physiquement éloignés. Il est également vulnérable aux attaques de proximité, lorsqu'un attaquant à proximité entend le code audio et l'utilise pour contourner l'authentification. Sound-Proof Karapanos *et al.* (2015) tente de résoudre ce problème en comparant les sons ambiants capturés par les microphones des deux appareils afin d'évaluer leur proximité. Bien qu'innovante, cette méthode reste vulnérable aux attaques de prédiction sonore, où un attaquant anticipe ou rejoue l'environnement sonore pour simuler la proximité Shrestha *et al.* (2016). De plus, Sound-Proof fonctionne mal dans des environnements calmes ou spacieux. SoundAuth Wang *et al.* (2018), une amélioration de Sound-Proof, diffuse des sons aléatoires proches de l'ultrason, difficiles à prédire, afin de vérifier la proximité. Ces signaux sont ensuite traités à l'aide de techniques d'apprentissage automatique pour prendre des décisions d'authentification. Cependant, ces fréquences restent perceptibles par les humains et les animaux domestiques, ce qui les rend inconfortables. En outre, SoundAuth est vulnérable aux attaques MiTM, où un adversaire relaie les sons du navigateur principal vers le téléphone. Listening Watch Shrestha & Saxena (2018) suit une logique similaire à SoundAuth, mais remplace le bruit ambiant par un message vocal aléatoire joué par le navigateur. Malgré cette amélioration, le système reste vulnérable aux attaquants disposant d'un accès temporaire à l'un des appareils : ils peuvent enregistrer, transmettre et rejouer le son près du second appareil, contournant ainsi le second facteur. Les modèles de menace de ces solutions considèrent souvent uniquement des attaquants distants et négligent les menaces locales. AlQahtani *et al.* (2024) exploite les signaux Wi-Fi et des modèles d'apprentissage automatique pour mettre en œuvre une authentification continue fondée sur les habitudes d'utilisation et le contexte environnemental. Toutefois, cette approche nécessite que les deux appareils soient connectés au même réseau Wi-Fi, ce qui limite sa portabilité dans des scénarios mobiles ou en itinérance.

Des méthodes plus sûres, basées sur la proximité, ont également été proposées. Han et al. utilisent des canaux ultrasoniques résistants aux attaques MiTM, grâce à l'unicité des

empreintes acoustiques Han *et al.* (2018). Ren et al. proposent la détection de proximité comme méthode d'authentification à deux facteurs en capturant des signaux sonores émis alternativement par les deux dispositifs légitimes, puis en réalisant une analyse de similarité sur la perte d'énergie au cours d'une période donnée Ren *et al.* (2021). PPGPass Cao *et al.* (2020) propose d'utiliser des capteurs de photopléthysmographie (PPG) portés au poignet pour valider l'identité de l'utilisateur.

L'article Atallah *et al.* (2021) introduit une solution d'accès hôtelier intelligent basée sur la technologie NFC (Near Field Communication), utilisant l'émulation de carte hôte pour une authentification transparente. Ces mécanismes visent à équilibrer sécurité et utilisabilité, tout en maintenant une forte résistance aux attaques et une grande précision de détection. La vulnérabilité des systèmes d'authentification continue basés sur le toucher (TCAS) face aux attaques adversariales actives est explorée dans Agrawal *et al.* (2022).

FIGURE 2.1 : Données environnementales.

2.2 APPROCHES BASÉES SUR DES DONNÉES COMPORTEMENTALES

D'autres méthodes 2FA s'appuient sur des caractéristiques comportementales uniques capturées par des objets connectés afin de mettre en œuvre une authentification continue Acar *et al.* (2019), Acar *et al.* (2020), Acar *et al.* (2021). De son côté, Shrestha *et al.* (2019) utilise les schémas de marche capturés via un smartphone et une montre connectée. Lamiche *et al.* (2019), propose une authentification continue sur smartphone basée sur des données biométriques comportementales comme la démarche et la dynamique de frappe. Les résultats démontrent une robustesse face à divers types d'attaques. Cependant, ces systèmes nécessitent des phases d'entraînement spécifiques à chaque utilisateur, ce qui complique leur généralisation. De plus, la variabilité inhérente au comportement humain constitue un défi à long terme.

2.3 APPROCHES BASÉES SUR IA ET DES DONNÉES COMPORTEMENTALES

Divers mécanismes d'authentification sécurisée exploitant l'apprentissage automatique (ML) ont été proposés pour différentes applications Kim *et al.* (2019), Aksu *et al.* (2018), Zhang & Zhang (2021), Lee & Lee (2017). Par exemple, Gupta et al. Gupta *et al.* (2023) ont proposé un mécanisme d'authentification sécurisé exploitant le ML et un système basé sur des valeurs aléatoires (nonces) pour un système d'information de télémédecine. Punithavathi et al. Punithavathi *et al.* (2019) ont introduit un système d'authentification biométrique annulable basé sur le cloud pour les objets connectés. Dans Abuhamad *et al.* (2020), les auteurs ont proposé une méthode d'authentification active fondée sur l'apprentissage profond qui utilise les capteurs des smartphones grand public pour authentifier les utilisateurs. De plus, Lee *et al.* (2019) a introduit une technique de protection des données des entrées souris qui génère des positions de curseur aléatoires afin de protéger les données de saisie, tout en utilisant le ML pour vérifier leur sécurité. Une nouvelle technique d'accès sécurisé aux smartphones basée sur

la dynamique de frappe, renforcée par une détection tactile piézoélectrique, a également été proposée dans Tang *et al.* (2022).

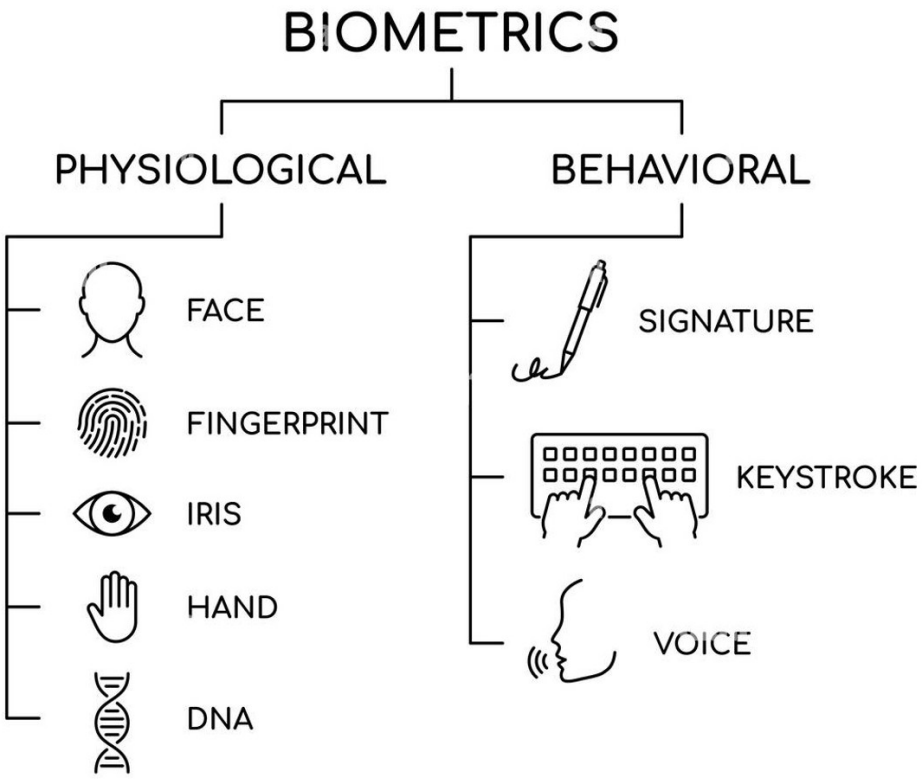


FIGURE 2.2 : Données comportementales et physiologiques.
Can & Atılgan (2023)

À la différence des travaux antérieurs, les approches existantes 2FA sans effort présentent encore plusieurs limites : les systèmes basés uniquement sur le BLE, tels qu'ABLE He *et al.* (2022), dépendent fortement de la densité des dispositifs environnants et deviennent inopérants dans les environnements dépourvus de signaux détectables, tandis que les solutions purement acoustiques comme Sound-Proof Karapanos *et al.* (2015) sont vulnérables aux attaques de relecture ou de prédiction sonore et échouent dans les environnements silencieux.

SBLE comble ce manque en adoptant une approche hybride combinant simultanément les caractéristiques des signaux BLE et de l'audio ambiant. Cette fusion permet d'améliorer la fiabilité de la détection de co-localisation, d'assurer une authentification plus robuste et réellement sans effort, et d'offrir une résilience accrue face aux attaquants distants ou co-localisés. De plus, la conception modulaire de SBLE le rend facilement intégrable dans les systèmes d'authentification continue modernes, tout en préservant la confidentialité des données utilisateurs.

CHAPITRE III

MODÈLES, HYPOTHÈSES ET CONCEPTS FONDAMENTAUX

Dans ce chapitre, nous détaillons les modèles et hypothèses sur lesquels repose SBLE, notamment les scénarios d'utilisation, les types d'attaques considérées et les contraintes de conception. Cette section rappelle également les concepts techniques nécessaires à la compréhension de notre approche, tels que les mécanismes d'analyse de signaux audio ambiants, des signaux BLE, et les métriques de similarité utilisées pour la détection de co-localisation et les principes du Bluetooth Low Energy.

3.1 MODÈLE DU SYSTÈME

Nous considérons le cas général d'une authentification par navigateur : un utilisateur tente d'accéder à un serveur web distant simplement en saisissant ses identifiants dans le navigateur de son ordinateur client. Son appareil de confiance, un smartphone (exécutant une application dédiée) placé à proximité de l'ordinateur assiste automatiquement l'authentification He *et al.* (2022), Karapanos *et al.* (2015). Notre système d'authentification à deux facteurs, repose sur trois entités réseau : un serveur d'authentification distant et deux appareils (un ordinateur client et un smartphone).

L'utilisateur emporte son smartphone partout avec lui et peut avoir besoin de se connecter au serveur depuis n'importe quel ordinateur client (par exemple, un ordinateur portable au bureau, un ordinateur de bureau à domicile ou une tablette dans un café). Dans tous les cas, nous supposons que l'ordinateur client et le smartphone sont chacun équipés de modules Bluetooth, ainsi que d'un haut-parleur et d'un microphone, qu'ils soient intégrés ou externes. Conformément au principe de 2FA sans effort, l'utilisateur n'a pas besoin d'installer de plugin

particulier sur son navigateur. Afin de clarifier notre modèle, nous supposons que les deux appareils utilisateurs, ainsi que le serveur web, sont exempts de logiciels malveillants. Le serveur web possède également un certificat TLS valide, permettant aux deux dispositifs d'établir des connexions Internet sécurisées avec lui.

Avant toute authentification à deux facteurs en ligne, l'utilisateur doit enregistrer (de manière hors bande, à l'aide de ses identifiants) son smartphone auprès du serveur. Cette étape permet, par exemple, d'associer la clé publique *pk* du téléphone au compte utilisateur, afin que le serveur puisse authentifier le smartphone enregistré et maintenir une communication sécurisée avec lui.

FIGURE 3.1 : Composants requis

3.2 MODÈLE DE MENACE

L'objectif d'un attaquant est d'accéder frauduleusement au service web. Dans la mesure où notre objectif est de concevoir un protocole 2FA sans effort, nous adoptons un modèle de menace similaire à celui proposé dans les travaux antérieurs Karapanos *et al.* (2015), He *et al.* (2022). Nous supposons que l'attaquant comprend le fonctionnement du système SBLE, mais ne peut pas compromettre simultanément les deux facteurs d'authentification, à savoir

les identifiants de la victime et l'application installée sur le téléphone enregistré. Dans le cas contraire, cette combinaison lui permettrait de contourner n'importe quel protocole 2FA.

Notre analyse se concentre donc sur la sécurité offerte par le second facteur d'authentification, c'est-à-dire le smartphone de confiance. Nous supposons ainsi que l'attaquant a déjà compromis les identifiants de la victime (premier facteur), que ce soit par des attaques de phishing, des fuites de bases de données de mots de passe, ou d'autres méthodes similaires. Cette hypothèse nous permet d'exclure le scénario dans lequel l'application mobile elle-même serait compromise.

Nous supposons également que le serveur est sécurisé et non compromis, car dans le cas contraire, tous les mécanismes d'authentification seraient rendus inefficaces. L'attaquant cherche donc à contourner le 2FA afin de se connecter au compte de la victime sur le serveur web. On suppose qu'il connaît le fonctionnement des systèmes 2FA basés sur les signaux audio et BLE, et qu'il est capable de collecter certaines informations personnelles sur la victime, telles que son adresse IP, son numéro de téléphone, ou sa localisation, afin de lancer des attaques à distance, qu'elles soient actives ou passives. Typiquement, ces attaques peuvent consister à déclencher activement la vibration du téléphone de la victime (attaque active), ou à attendre passivement qu'il vibre naturellement, tout en envoyant des sons prévisibles au navigateur pour simuler un environnement audio similaire. L'attaquant peut également exploiter la localisation de la victime pour prédire les dispositifs sans fil à proximité et simuler un environnement BLE cohérent.

Une attaque est considérée comme réussie si l'attaquant parvient à prouver la possession du second facteur, c'est-à-dire à simuler la présence du dispositif légitime. Cependant, nous démontrons que SBLE peut contrer efficacement de telles attaques en s'appuyant sur la

randomisation des adresses BLE (BD_ADDR) et sur la variabilité instantanée des valeurs RSSI.

Par ailleurs, un attaquant co-localisé pourrait tenter de se connecter à la place de l'utilisateur en exploitant un environnement audio et BLE très similaire. Néanmoins, nous soutenons que de telles attaques ciblées sont difficiles à réaliser dans le cadre de SBLE, car obtenir des données BLE suffisamment similaires nécessiterait une proximité physique extrêmement étroite, moins de 50 centimètres entre l'attaquant et le dispositif légitime.

Enfin, les attaques de MitM et les attaques par déni de service (DoS) ne sont pas abordées dans ce mémoire. Nous considérons deux types d'attaquants : ceux présents physiquement à proximité de la victime ; et ceux situés à distance.

3.3 CONCEPTS FONDAMENTAUX

Dans cette partie, nous présentons les concepts fondamentaux nécessaires à la compréhension de notre étude empirique. Plus précisément, nous analysons les différentes métriques utilisées pour déterminer la similarité entre deux échantillons audio, ainsi que la similarité des adresses `BD_ADDR` et des mesures RSSI dans deux enregistrements dans un contexte BLE.

3.3.1 FONDEMENTS SUR LE CALCUL DE LA SIMILARITÉ AUDIO

Le problème consistant à déterminer la similarité entre deux échantillons audio dans SBLE est similaire à celui abordé dans Sound-Proof Karapanos *et al.* (2015). Dans ce dernier, les auteurs comparent deux échantillons quasi-alignés (avec un décalage temporel inférieur à 150 ms), ce qui permet d'extraire des informations pertinentes non seulement de leur représentation fréquentielle, mais également de leur représentation temporelle. Afin de prendre

en compte à la fois les caractéristiques temporelles et fréquentielles des enregistrements, ils utilisent un filtrage en bandes d'un tiers d'octave ainsi qu'une corrélation croisée.

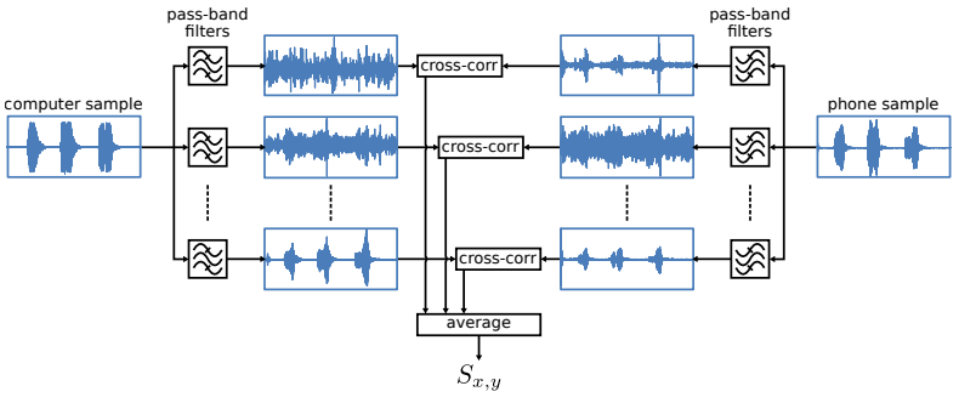


FIGURE 3.2 : Schéma fonctionnel du module calculant le score de similarité entre deux échantillons.

Karapanos *et al.* (2015)

Le calcul s'effectue sur le téléphone. Si $S_{x,y} > \tau_C$ et que la puissance moyenne des échantillons est supérieure à τ_{dB}, le téléphone considère la tentative de connexion comme légitime

Bandes d'un tiers d'octave

Les bandes d'octave divisent la plage audible des fréquences (environ de 20 Hz à 20 kHz) en 11 bandes non chevauchantes, où le rapport entre la fréquence la plus élevée et la plus basse d'une bande est de 2 pour 1. Chaque octave est représentée par sa fréquence centrale, et la fréquence centrale d'une octave donnée est le double de celle de l'octave précédente. Les bandes d'un tiers d'octave divisent les dix premières bandes d'octave en trois parties et la dernière en deux, ce qui donne un total de 32 bandes. Ces bandes sont largement utilisées

en acoustique, et leurs plages de fréquences ont été normalisées Karapanos *et al.* (2015). La fréquence centrale de la bande la plus basse est de 16 Hz (couvrant de 14,1 Hz à 17,8 Hz), tandis que la fréquence centrale de la bande la plus haute est de 20 kHz (couvrant de 17,780 Hz à 22,390 Hz).

Dans la suite, nous notons $B = [lb - hb]$ un ensemble de bandes d'un tiers d'octave contiguës, allant de la bande dont la fréquence centrale est lb Hz à celle dont la fréquence centrale est hb Hz.

Le découpage d'un signal en bandes d'un tiers d'octave permet d'obtenir une information à haute résolution fréquentielle sur le signal original tout en préservant sa représentation temporelle.

Corrélation croisée

La corrélation croisée est une mesure standard de similarité entre deux séries temporelles. Soient x et y deux signaux représentés sous forme de séries temporelles discrètes de n points. La corrélation croisée $c_{x,y}(l)$ mesure leur similarité en fonction du décalage $l \in [0, n-1]$ appliqué à y :

$$c_{x,y}(l) = \sum_{i=0}^{n-1} x(i) \cdot y(i-l)$$

, où $y(i) = 0$ si $i < 0$ ou $i > n-1$.

Pour tenir compte des différences d'amplitude entre les deux signaux, la corrélation croisée peut être normalisée comme suit :

$$\tilde{c}_{x,y}(l) = \frac{c_{x,y}(l)}{\sqrt{c_{x,x}(0) \cdot c_{y,y}(0)}}$$

où $c_{x,x}(l)$ et $c_{y,y}(l)$ représentent respectivement les auto-corrélations de x et y.

Cette normalisation projette la valeur de $\tilde{c}_{x,y}(l)$ dans l'intervalle $[-1,1]$. Une valeur de $\tilde{c}_{x,y}(l) = 1$ indique qu'au décalage l, les deux signaux ont la même forme (même si leurs amplitudes diffèrent), tandis qu'une valeur de $\tilde{c}_{x,y}(l) = -1$ signifie qu'ils ont la même forme mais des signes opposés. Une valeur de $\tilde{c}_{x,y}(l) = 0$ indique que les deux signaux sont non corrélés.

Si le décalage réel entre les deux signaux est inconnu, on peut ignorer l'information de signe et utiliser la valeur absolue de la corrélation croisée maximale :

$$\hat{c}_{x,y}(l) = \max_{l} \left(|c'_{x,y}(l)| \right)$$

comme métrique de similarité, où $0 \leq \hat{c}_{x,y}(l) \leq 1$.

La charge de calcul associée à la corrélation croisée $c_{x,y}(l)$ peut être réduite en appliquant le théorème de la corrélation croisée, en calculant :

$$c_{x,y}(l) = \mathscr{F}^{-1} \left(\mathscr{F}(x)^* \cdot \mathscr{F}(y) \right)$$

où $\mathscr{F}$ désigne la transformée de Fourier discrète (DFT), et l'astérisque * représente le conjugué complexe Karapanos *et al.* (2015).

Soit x_i la composante du signal correspondant à la i-ème bande d'un tiers d'octave du signal x. Le score de similarité est alors défini comme la moyenne des corrélations croisées maximales calculées sur les paires de composantes x_i, y_i Karapanos *et al.* (2015) :

$$S_{x,y} = \frac{1}{n} \sum_{i=1}^{n} \hat{c}_{x_i,y_i}(\ell)$$

où ℓ est borné entre 0 et $\ell_{\max}$.

La figure 4.14 présente un schéma fonctionnel détaillant le calcul de ce score de similarité.

3.3.2 FONDEMENTS SUR LE CALCUL DE LA SIMILARITÉ DES SIGNAUX BLE

Nous retenons deux métriques pour évaluer la similarité des **adresses BD_ADDR** et des mesures **RSSI** dans deux enregistrements. Nous définissons deux dispositifs utilisateurs, notés A et B. Soient S_a et S_b les deux ensembles d'enregistrements obtenus par ces appareils, et n_a et n_b le nombre de dispositifs BLE observés par chacun d'eux. Pour chaque dispositif BLE d'un enregistrement, soient m et r respectivement son **adresse BD_ADDR** et la moyenne de ses mesures RSSI. Nous définissons les ensembles suivants :

$$
\begin{aligned}
S_a &= \left\{ \left(m_i^{(a)}, r_i^{(a)} \right) \mid i \in \mathbb{Z}_{n_a} \right\}, \\
S_b &= \left\{ \left(m_i^{(b)}, r_i^{(b)} \right) \mid i \in \mathbb{Z}_{n_b} \right\}, \\
S_\cap &= \left\{ (m, r^{(a)}, r^{(b)}) \mid (m, r^{(a)}) \in S_a, (m, r^{(b)}) \in S_b \right\}, \\
S_a^{(m)} &= \{ m \mid (m, r) \in S_a \}, \quad S_b^{(m)} = \{ m \mid (m, r) \in S_b \}, \\
S_\cap^{(m)} &= S_a^{(m)} \cap S_b^{(m)}, \quad S_\cup^{(m)} = S_a^{(m)} \cup S_b^{(m)}.
\end{aligned}
$$

Indice de Jaccard

Nous utilisons l'indice de Jaccard pour mesurer la similarité des adresses **BD_ADDR** enregistrées par A et B :

$$
s_j(A, B) = \frac{|S_\cap^{(m)}|}{|S_\cup^{(m)}|} \in [0, 1]
$$

Cet indice permet d'identifier les attaquants distants lançant une attaque d'imitation en devinant ou en préenregistrant des signaux BLE dans le contexte de l'utilisateur. Cependant, il s'avère insuffisant pour détecter les attaquants co-présents, car chaque appareil BLE environnant peut être perçu par leur appareil de connexion.

De plus, la similarité rapportée par s_j peut être trop grossière. En effet, lorsque la distance entre A et B ne varie pas de manière significative, s_j reste inchangé. Pour remédier à cela, dans *ABLE* He *et al.* (2022), les auteurs ont utilisé deux métriques pour identifier efficacement les attaquants co-présents lorsque s_j augmente. Ils ont d'abord employé le coefficient de corrélation de Pearson pour vérifier la similarité des mesures RSSI entre A et B.

Cependant, celui-ci s'est révélé insuffisant pour déterminer la similarité entre deux valeurs RSSI, car il ne prend pas en compte l'amplitude des données RSSI. Pour résoudre ce problème, ils He *et al.* (2022) ont adopté la distance euclidienne normalisée. Néanmoins, cette métrique devient inadaptée lorsque peu de dispositifs BLE sont détectés (par exemple, ≤ 2), ce qui limite leur étude.

Corrélation croisée maximale

Pour surmonter ces limitations, nous proposons d'utiliser la *corrélation croisée maximale* appliquée aux séries temporelles RSSI extraites à intervalles réguliers (par exemple, 100 ms) sur une fenêtre temporelle T (par exemple, 3000 ms).

Chaque signal BLE est transformé en un vecteur de la forme :

$$X = [x_0, x_1, \ldots, x_{n-1}] \quad \text{où} \quad n = \frac{T}{\text{intervalle}}$$

avec :

— x_i : valeur RSSI à l'instant $t = i \cdot \text{intervalle}$,

— valeur par défaut : -70 dBm si aucune mesure n'est reçue à cet instant.

Soit $S_{\cap}^{(m)}$ l'ensemble des adresses MAC détectées par les deux appareils. Pour chaque adresse $m \in S_{\cap}^{(m)}$, nous construisons :

$$X^{(m)} = [x_0^{(m)}, \ldots, x_{n-1}^{(m)}] \quad \text{pour l'appareil A}$$

$$Y^{(m)} = [y_0^{(m)}, \ldots, y_{n-1}^{(m)}] \quad \text{pour l'appareil B}$$

Le score de similarité des valeurs RSSI entre A et B est ensuite calculé comme suit :

$$S_c(A,B) = \frac{1}{|S_{\cap}^{(m)}|} \sum_{m \in M} \max_{-L \leq \ell \leq L} \left(\frac{\left| \sum_{i=0}^{n-1} x_i^{(m)} \cdot y_{i+\ell}^{(m)} \right|}{\sqrt{\left(\sum_{i=0}^{n-1} (x_i^{(m)})^2 \right) \left(\sum_{i=0}^{n-1} (y_{i+\ell}^{(m)})^2 \right) + \varepsilon}} \right)$$

où :

— $x_i^{(m)}$: valeur RSSI de l'appareil A pour l'adresse m à l'instant i,

— $y_{i+\ell}^{(m)}$: valeur RSSI de l'appareil B pour l'adresse m avec un décalage temporel ℓ,

— L : décalage temporel maximal (par exemple, ± 3 pour 100 ms $\rightarrow \pm 300$ ms),

— $\varepsilon = 10^{-9}$: petite constante pour éviter la division par zéro,

— ℓ : décalage temporel entre les deux séries.

Ce score capture à la fois la forme et l'intensité du signal RSSI, tout en tolérant de légers désalignements temporels entre les mesures. En moyennant sur toutes les adresses m, nous obtenons un score global plus robuste permettant de distinguer les appareils proches mais distincts.

3.3.3 NOTIONS SUR LES SIGNAUX SANS FIL

NATURE SENSIBLE À LA LOCALISATION DES SIGNAUX SANS FIL

La répartition des dispositifs sans fil et l'atténuation des signaux radio font qu'un emplacement est unique et distinct d'un autre. En d'autres termes, le signal sans fil est *sensible à la localisation*. Lorsque deux appareils sont physiquement proches (par exemple, à une distance inférieure à une demi-longueur d'onde), les caractéristiques des signaux sans fil environnementaux qu'ils captent sont similaires, puisqu'ils se trouvent approximativement au même endroit. En revanche, lorsqu'ils sont éloignés, les caractéristiques des signaux collectés diffèrent significativement He *et al.* (2022).

ADRESSE BD_ADDR DANS LE BLE

Comparé au Bluetooth classique, le *Bluetooth Low Energy* (BLE) introduit un mécanisme de sécurité basé sur la randomisation des adresses afin d'empêcher le pistage des appareils. Les dispositifs BLE peuvent utiliser soit l'adresse MAC fixe fournie par le fabricant, soit une adresse aléatoire optionnelle comme adresse de publicité (`BD_ADDR`). Le sous-type spécifique d'une adresse aléatoire peut être l'un des suivants He *et al.* (2022) :

— **Adresse statique :** elle change aléatoirement après chaque cycle d'alimentation ou reste inchangée en permanence.

— **Adresse privée non résoluble :** elle est générée de manière aléatoire et change périodiquement (toutes les 15 minutes, selon les recommandations).

— **Adresse privée résoluble :** elle est générée à l'aide d'une clé de résolution d'identité (*Identity Resolving Key*) et d'un nombre aléatoire, et change également périodiquement.

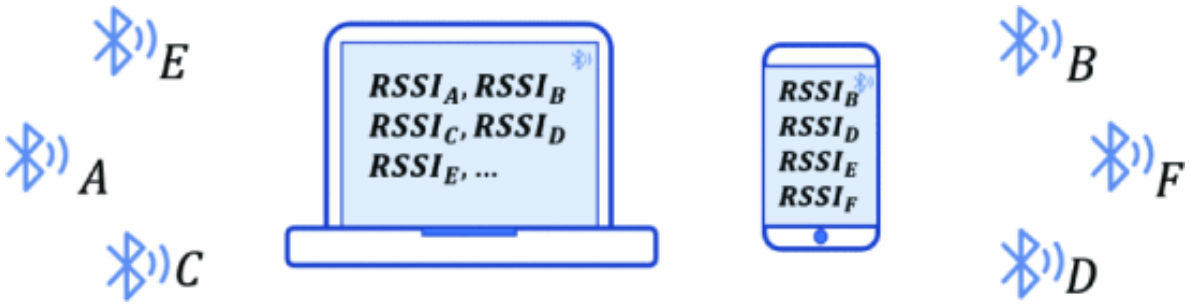


FIGURE 3.3 : Détection de colocalisation entre deux appareils utilisateurs

He *et al.* (2022)

CHAPITRE IV
ARCHITECTURE ET IMPLÉMENTATION DE SBLE

Ce chapitre décrit l'architecture globale du système SBLE, en détaillant les interactions entre ses composants : le serveur d'authentification, l'application mobile Android, et le module web. L'implémentation pratique est ensuite présentée, notamment le développement du serveur avec Flask, la communication sécurisée via TLS, et la gestion des enregistrements BLE et audio. Ce chapitre met également en avant les mécanismes de synchronisation temporelle et de chiffrement assurant la fiabilité et la confidentialité des échanges.

4.1 ARCHITECTURE

Le deuxième facteur d'authentification dans **SBLE** repose sur la vérification de la proximité physique du smartphone de l'utilisateur avec l'ordinateur utilisé pour la connexion. Cette proximité est évaluée en calculant un score de similarité entre les signaux audio ambiants capturés par les microphones des deux appareils, ainsi que deux scores de similarité entre les signaux BLE collectés par leurs modules Bluetooth respectifs.

Afin de préserver la vie privée de l'utilisateur, les échantillons audio et BLE bruts ne sont jamais transmis directement au serveur. Dans notre conception, le navigateur chiffre les enregistrements audio et BLE à l'aide d'une clé symétrique aléatoire générée à chaque session de connexion selon l'algorithme AES-256. Cette clé symétrique est ensuite chiffrée à l'aide de la clé publique du smartphone enregistré, conformément au protocole RSA-2048. Ces échantillons chiffrés sont ensuite transmis au smartphone via le serveur.

Lors de la réception des données chiffrées, le smartphone déchiffre les échantillons et calcule trois scores de similarité : l'un pour l'audio (comparant l'audio reçu à son propre

enregistrement local), et les deux autres pour les signaux BLE (comparant les empreintes BLE des deux appareils). Le smartphone détermine ensuite si les deux appareils sont effectivement co-localisés sur la base de ces scores, et envoie uniquement une décision binaire (co-localisé ou non) au serveur.

Il est important de noter que le smartphone ne partage jamais ses propres données audio ou BLE brutes avec le serveur. Toutes les communications entre l'ordinateur et le smartphone transitent par le serveur, mais aucune donnée environnementale sensible ne quitte les appareils de l'utilisateur sans être chiffrée.

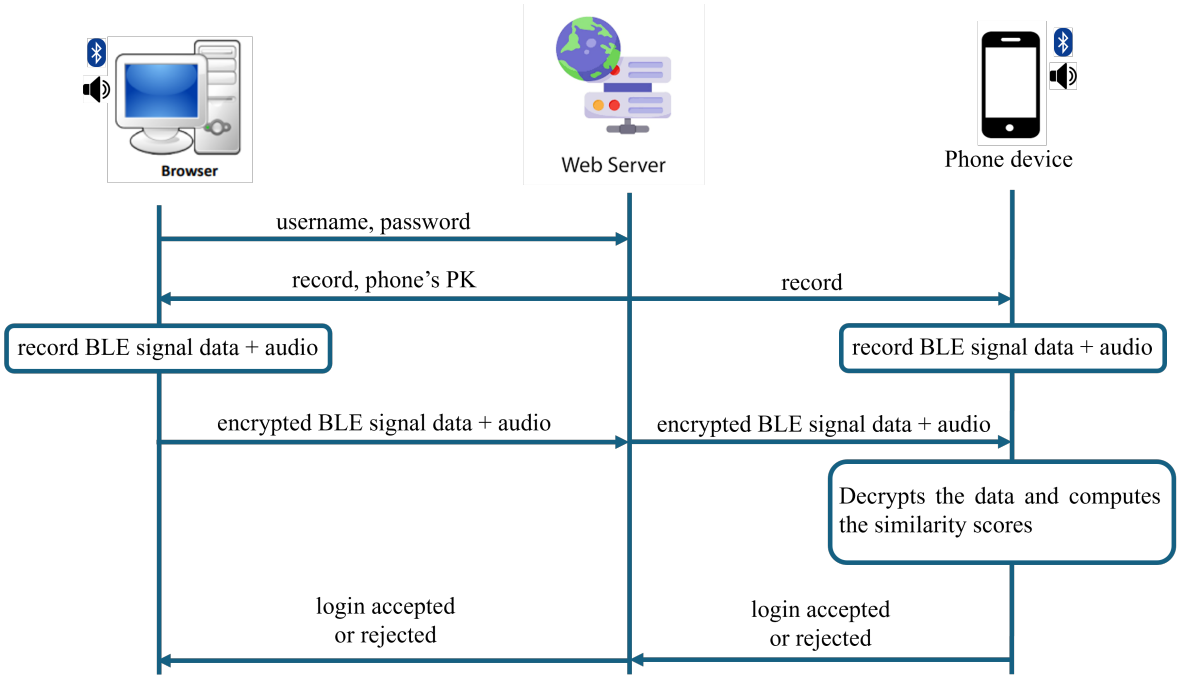


FIGURE 4.1 : Vue d'ensemble de l'authentification SBLE.

Lors de la connexion, le téléphone et l'ordinateur enregistrent simultanément le bruit ambiant à l'aide de leurs microphones, ainsi que les signaux BLE environnants via leurs modules Bluetooth respectifs. Le téléphone calcule les scores de similarité pour chaque type

de donnée (audio et BLE) en comparant les échantillons reçus avec ceux enregistrés localement. Il détermine ensuite le résultat sur la base de ces scores et l'envoie au serveur.

4.1.1 ENRÔLEMENT ET CONNEXION

Comme d'autres mécanismes d'authentification à deux facteurs basés sur des jetons logiciels, **SBLE** nécessite l'installation d'une application sur le téléphone de l'utilisateur, ainsi que son association avec le compte utilisateur sur le serveur.

Cette opération, effectuée une seule fois, peut être réalisée en utilisant des techniques d'enrôlement de jetons logiciels existantes Karapanos *et al.* (2015). On suppose qu'à la fin de la procédure d'enrôlement, le serveur a reçu la clé publique unique de l'application installée sur le téléphone de l'utilisateur et l'a associée au compte correspondant.

La Figure 4.1 présente une vue d'ensemble de la procédure de connexion.

- L'utilisateur ouvre un navigateur Web, accède à l'URL du serveur et saisit son nom d'utilisateur et son mot de passe ;
- Le serveur récupère ensuite la clé publique associée au téléphone de l'utilisateur et la transmet au navigateur ;
- Le navigateur et le téléphone démarrent alors simultanément un enregistrement audio et BLE d'une durée de t secondes, à l'aide de leurs microphones et modules Bluetooth respectifs. Durant cette phase, les deux appareils synchronisent leurs horloges avec le serveur. Une fois l'enregistrement terminé, chaque appareil ajuste les horodatages de ses échantillons en tenant compte du décalage d'horloge avec le serveur ;
- Le navigateur chiffre les échantillons audio et BLE à l'aide de la clé publique du téléphone, puis les envoie à ce dernier via le serveur, comme illustré à la Figure 4.2 ;

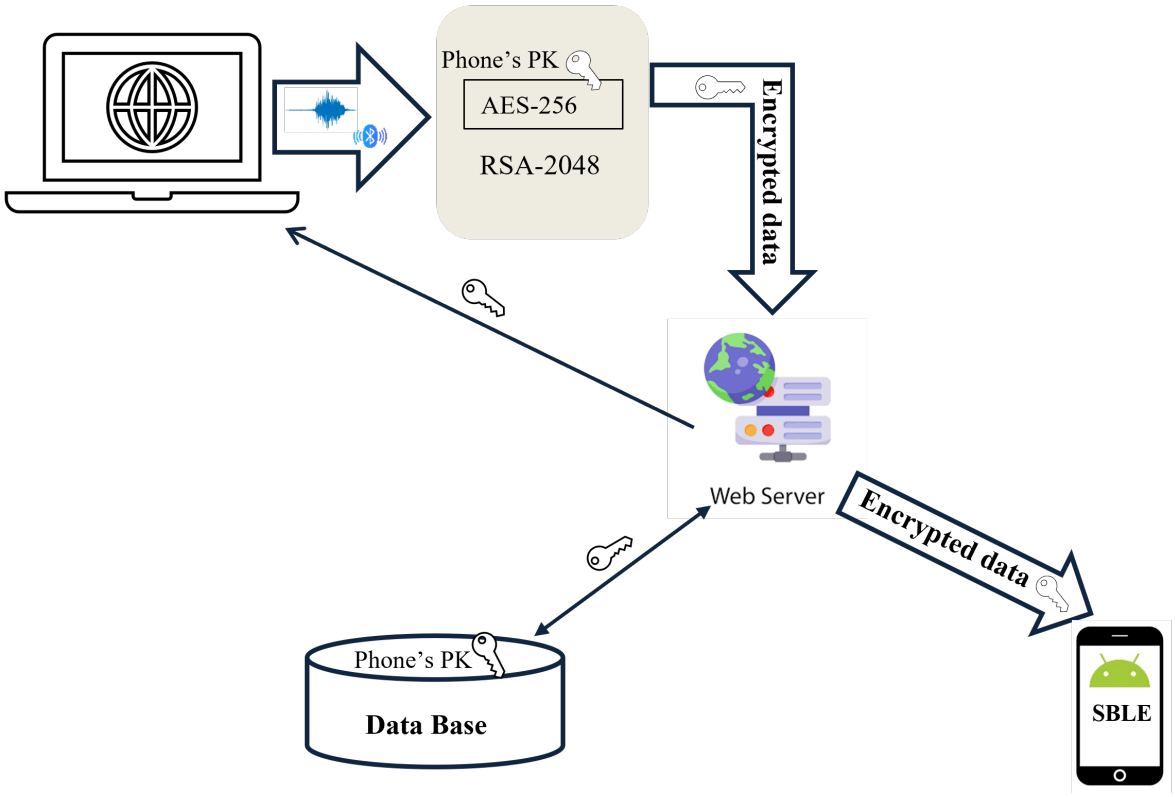


FIGURE 4.2 : Chiffrement des données par le navigateur, ainsi que leur transfert vers le serveur, puis du serveur vers l'application mobile.

- Le téléphone déchiffre les échantillons et les compare à ses propres échantillons enregistrés localement, en calculant les scores de similarités entre les échantillons de même type, en considerant un décalage temporel ;
- Si les scores de similarité audio et BLE dépassent leurs seuils respectifs τ_C, τ_B et τ_j, le téléphone conclut qu'il est effectivement co-localisé avec l'ordinateur et informe le serveur que la tentative de connexion est légitime, et ce dernier accorde l'accès. Dans le cas contraire l'accès reste vérouiller.

Ce processus est totalement transparent pour l'utilisateur, que l'environnement soit suffisamment bruyant ou silencieux.

4.1.2 CARACTÉRISTIQUES DU SYSTÈME PROPOSÉ

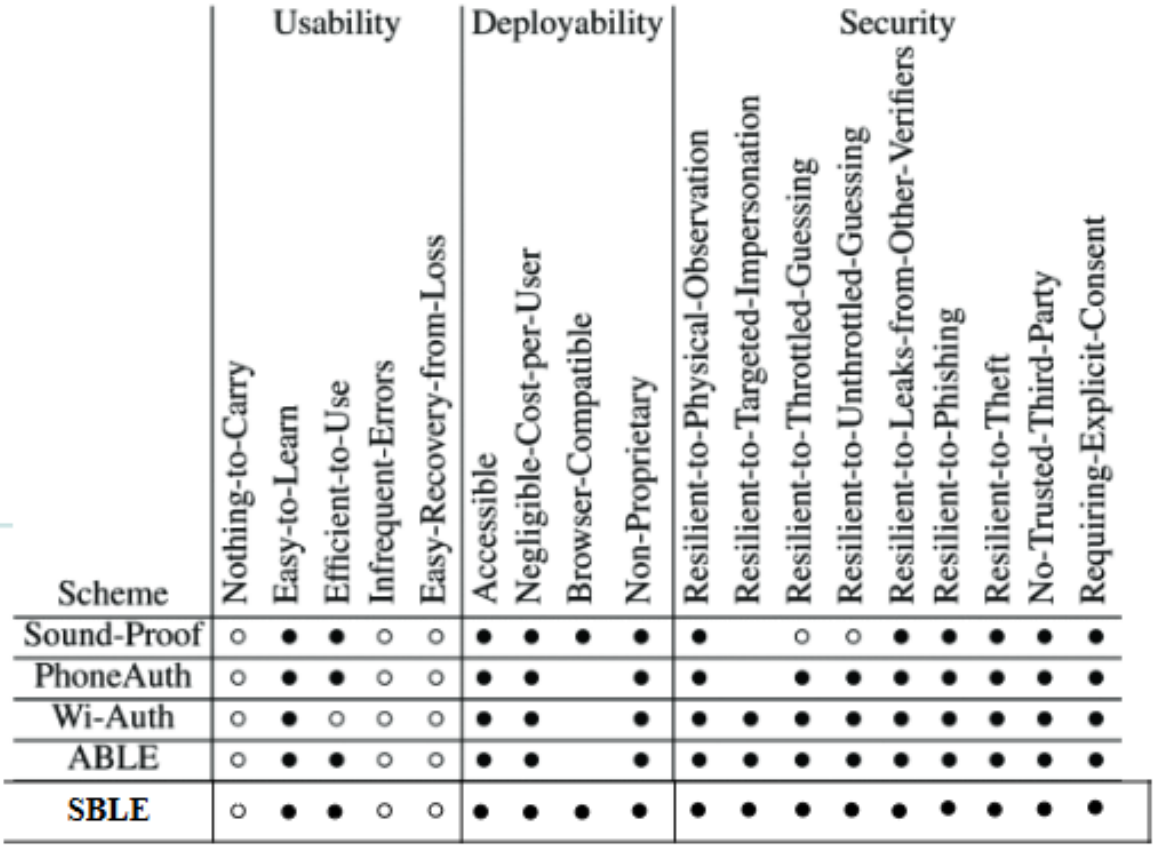
Dans cette partie, nous expliquerons les caractéristiques de notre système 2FA.

ZÉRO EFFORT

Le système proposé intègre une fonctionnalité « sans effort » ou « non interactive », qui améliore considérablement l'expérience utilisateur en automatisant le processus d'authentification et en éliminant toute saisie ou action supplémentaire. Le système met en œuvre efficacement la seconde couche d'authentification et vérifie leur identité (étapes 3 à 6). Cette approche fluide renforce non seulement la satisfaction des utilisateurs, mais aussi la sécurité en réduisant les risques d'erreur humaine, pour une expérience d'authentification simplifiée et sécurisée.

AUTHENTIFICATION CONTINUE

La fonction d'authentification continue du système SBLE renforce la sécurité en vérifiant de manière constante l'identité de l'utilisateur durant l'accès aux ressources protégées. Le serveur déclenche périodiquement (toutes les dix minutes) un processus de vérification pendant que l'utilisateur est connecté et interagit avec le site web. À chaque intervalle, le système enregistre de nouveaux échantillons des signaux audio et BLE, puis analyse leurs caractéristiques environnementales afin de confirmer la proximité effective entre le smartphone et le poste de travail. Si les appareils ne sont plus co-localisés, la session est immédiatement interrompue. Cette approche améliore non seulement la sécurité en empêchant les accès non autorisés après le départ de l'utilisateur, mais elle garantit également un confort d'utilisation



	Usability					Deployability				Security								
Scheme	Nothing-to-Carry	Easy-to-Learn	Efficient-to-Use	Infrequent-Errors	Easy-Recovery-from-Loss	Accessible	Negligible-Cost-per-User	Browser-Compatible	Non-Proprietary	Resilient-to-Physical-Observation	Resilient-to-Targeted-Impersonation	Resilient-to-Throttled-Guessing	Resilient-to-Unthrottled-Guessing	Resilient-to-Leaks-from-Other-Verifiers	Resilient-to-Phishing	Resilient-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent
Sound-Proof	○	●	●	○	○	●	●	●	●	●		○	○	●	●	●	●	●
PhoneAuth	○	●	●	○	○	●	●		●	●		●	●	●	●	●	●	●
Wi-Auth	○	●	○	○	○	●	●		●	●	●	●	●	●	●	●	●	●
ABLE	○	●	●	○	○	●	●		●	●	●	●	●	●	●	●	●	●
SBLE	○	●	●	○	○	●	●	●	●	●	●	●	●	●	●	●	●	●

FIGURE 4.3 : Comparaison de SBLE avec plusieurs systèmes existants.

optimal, en éliminant le besoin de déconnexion manuelle et en offrant une expérience fluide et sécurisée.

FLEXIBILITÉ

SBLE se distingue par sa compatibilité multi-plateforme et sa capacité à s'adapter à divers environnements et appareils. Il fonctionne avec la majorité des smartphones modernes

(Android) et des navigateurs web courants, sans nécessiter de matériel spécialisé ni de modification du système d'exploitation. De plus, son architecture modulaire lui permet de s'intégrer facilement à d'autres systèmes d'authentification ou infrastructures existantes (serveurs web, applications d'entreprise, systèmes de contrôle d'accès). Cette flexibilité fait de SBLE une solution hautement adaptable et évolutive.

SÉCURITÉ

SBLE résiste aux usurpations d'identité ciblées grâce à la nature géolocalisée du signal sans fil. De plus, il est résistant face aux attaques par imitation, face aux attaques par prédiction sonore et est imunisé face aux attaques à distance

4.2 IMPLÉMENTATION

Dans cette section, nous décrivons la mise en œuvre du schéma **SBLE**, qui se compose de quatre phases :

- Structure du site web ;
- L'application mobile ;
- Enregistrement des Signaux BLE et du Son Ambiant ;
- Analyse des signaux audio et BLE ;

4.2.1 ENVIRONNEMENT DE TRAVAIL

Environnement matériel

Pour le développement de notre serveur web et de notre application mobile, nous avons utilisé des ordinateurs portable Lenovo et HP avec la description ci-dessous :

— Processeur : Intel core i7

— Mémoire RAM : 8 Go

— Type du système : Système d'exploitation windows 64 bits

— Mémoire ROM : 1 To

Environnement logiciel

- **Visual studio code** est un éditeur de code extensible développé par Microsoft pour Windows, Linux et MacOs. Les fonctionnalités incluent la prise en charge du débogage, la mise en évidence de la syntaxe, la complétion intelligente du code, les snippets, la refactorisation du code et Git intégré. [1]
- **Android Studio** est un environnement de développement intégré (IDE) conçu par Google pour créer des applications Android. C'est l'outil officiel utilisé par les développeurs pour écrire, tester et déboguer des applications destinées aux téléphones et tablettes Android [2]
- **Ngrok** ngrok est un outil qui permet de rendre accessible un serveur local sur Internet. Autrement dit, il crée un tunnel sécurisé entre ton ordinateur et une URL publique temporaire, que tu peux partager pour tester une application web, une API ou une application mobile sans avoir besoin d'un hébergement. [3]
- **Github** est une plateforme en ligne qui permet aux développeurs de stocker, partager et collaborer sur du code source. Elle repose sur le système de contrôle de version Git, qui enregistre toutes les modifications apportées à un projet et facilite le travail en équipe.

1. Source : VSC
2. Source : Android-Studio
3. Source : Ngrok.org

En d'autres termes, GitHub est comme un "cloud pour le code" où plusieurs personnes peuvent travailler sur le même projet sans écraser le travail des autres. [4]

FIGURE 4.4 : Environnements de développement.

Outils de développement

- **Java** est un langage de programmation orienté objet , généraliste et sûr en mémoire . Il est conçu pour être portable, sécurisé, et indépendant de la plateforme, grâce au principe "Write Once, Run Anywhere" (WORA), ce qui signifie que le code Java compilé peut s'exécuter sur toutes les plateformes compatibles Java sans nécessiter de recompilation. [5]

4. Source : github.org
5. Source : Java

- **Flask** est un framework web minimaliste écrit en Python. Il permet de créer facilement des applications web et des API REST. Flask est dit micro-framework car il ne contient que les composants essentiels (serveur web, routage, gestion des requêtes/réponses), tout en laissant la liberté d'ajouter les extensions nécessaires (base de données, authentification, etc.) [6]
- **Javascript** est un langage informatique utilisé sur les pages web. Ce langage à la particularité de s'activer sur le poste client, en d'autres mots c'est votre ordinateur qui va recevoir le code et qui devra l'exécuter. C'est en opposition à d'autres langages qui sont activé côté serveur. L'exécution du code est effectuée par les navigateurs internets [7]
- **HTML** est le langage de balisage standard utilisé pour structurer et afficher le contenu des pages web. Il ne s'agit pas d'un langage de programmation, mais d'un langage de description qui indique au navigateur comment organiser et présenter les éléments d'une page. [8]
- **MySQL** est un Système de Gestion de Base de Données Relationnelle (SGBDR) fondé sur le langage SQL (Structured Query Language).Il permet de stocker, organiser, gérer et interroger des données structurées sous forme de tables. MySQL est open-source, rapide et largement utilisé pour les applications web, souvent associé à PHP ou à des frameworks comme Flask ou Django. [9]

6. Source : Flask.org
7. Source : Javascript
8. Source : Html.org
9. Source : MySQL

FIGURE 4.5 : Outils de développement.

4.2.2 SYNCHRONISATION DE L'HORLOGE Wang *et al.* (2018)

Les horloges des systèmes informatiques peuvent être synchronisées à l'aide du *Network Time Protocol* (NTP), dans lequel un client envoie une requête à un serveur et reçoit une réponse en retour. Soient t_0, t_1, t_2 et t_3 les horodatages locaux du client et du serveur correspondant respectivement à : l'envoi de la requête, la réception de la requête, l'envoi de la réponse et la réception de la réponse.

On suppose que l'heure locale du serveur est θ lorsque l'heure locale du client est 0. Soit δ le délai aller-retour (*round-trip delay*). Idéalement, on a :

$$t_1 = t_0 + \theta + \frac{\delta}{2} \quad \text{et} \quad t_3 = t_2 + \theta + \frac{\delta}{2}.$$

Ainsi, les expressions du décalage d'horloge (θ) et du délai aller-retour (δ) sont données par :

$$\theta = \frac{(t_1 - t_0) - (t_3 - t_2)}{2}, \qquad \delta = (t_1 + t_3) - (t_0 + t_2).$$

4.2.3 STRUCTURE DU SITE WEB

Le site web est construit avec le framework MVC (Modèle–Vue–Contrôleur).

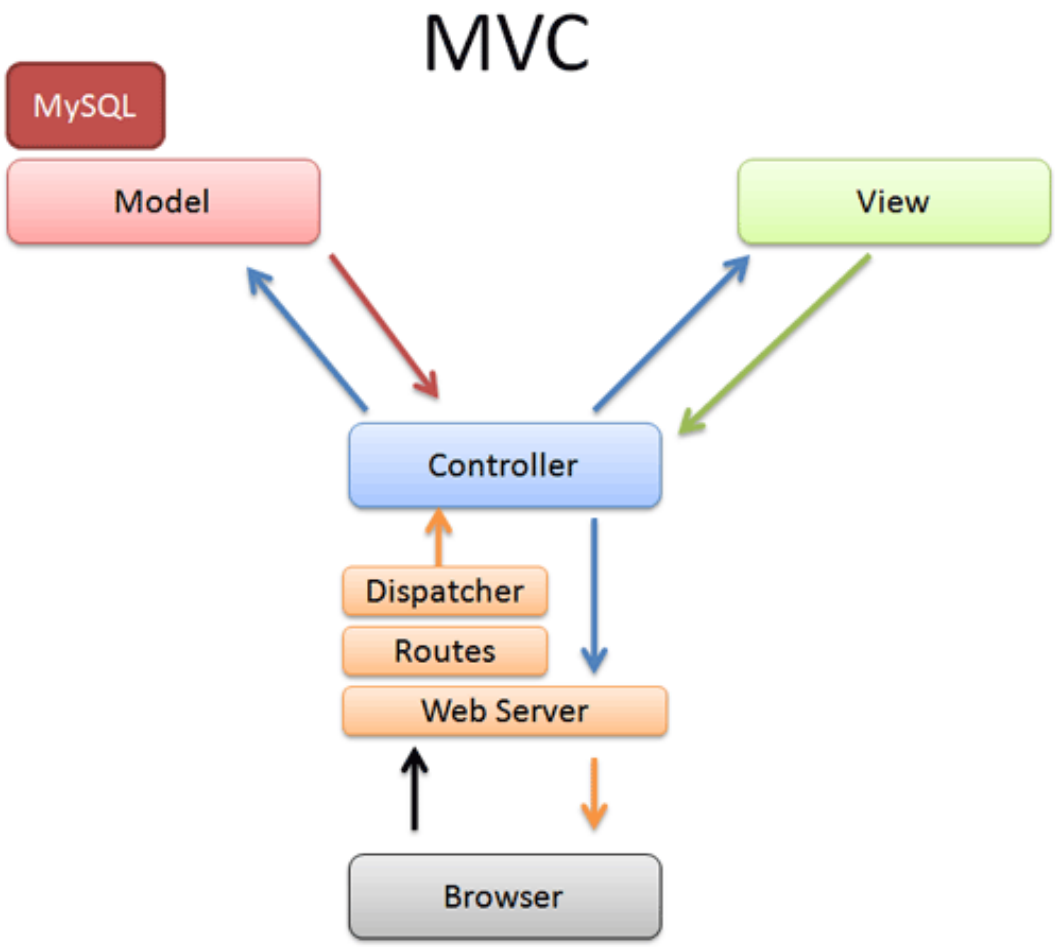


FIGURE 4.6 : Diagramme MVC

Stackoverflow (2025)

C'est un modèle d'architecture logicielle utilisé pour séparer la logique métier, l'interface utilisateur et le contrôle des interactions dans une application.

- **Modèle** : Gère les données, la logique métier et les règles de l'application. ;
- **Vue** : Gère l'affichage et la présentation des données à l'utilisateur.
- **Contrôleur** : Fait le lien entre la vue et le modèle : il intercepte les actions de l'utilisateur, met à jour le modèle, et choisit la vue à afficher.

Demande de Connexion

Le composant du navigateur permettant aux utilisateurs d'envoyer leurs demandes de connexion est implémenté en `HTML` et `JavaScript`, tandis que la partie serveur est développée à l'aide du framework `Flask` en `Python`, avec une base de données `MySQL`.

Une `API REST Flask` est utilisée pour établir une connexion bidirectionnelle et transférer les données entre le navigateur et le serveur.

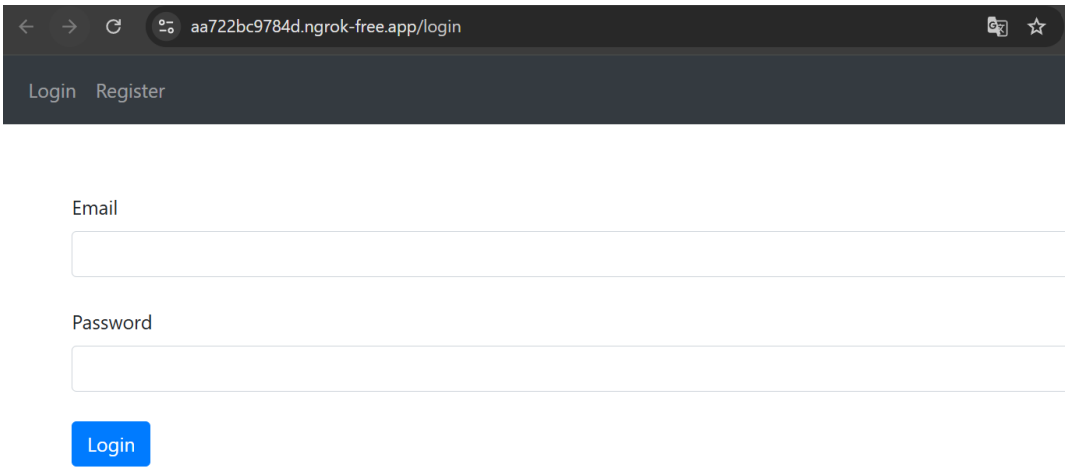


FIGURE 4.7 : Page de connexion.

FIGURE 4.8 : Lancement du serveur Flask http.

4.2.4 APPLICATION MOBILE

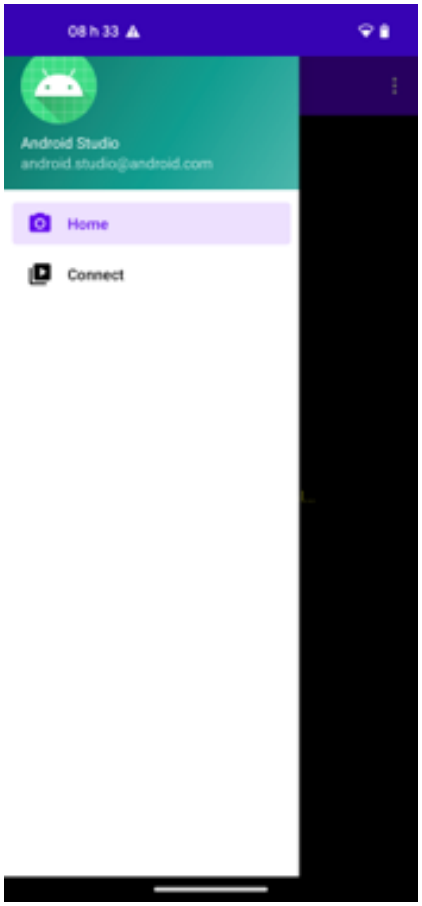


FIGURE 4.9 : Menu de l'application mobile.

Côté téléphone, nous avons implémenté une application `Android` agissant comme un jeton logiciel (*software token*). Elle s'exécute en arrière-plan et reste inactive jusqu'à ce qu'elle reçoive une notification de synchronisation du serveur, transmise par une requête `GET` régulièrement sondée via l'API Flask. Dès que l'utilisateur saisit ses identifiants, la clé publique du smartphone associée à son compte est récupérée afin d'établir l'association et d'envoyer la notification d'enregistrement au téléphone. L'API `BluetoothLeScanner` est utilisée pour enregistrer les signaux BLE, tandis que l'API `MediaRecorder` capture le son ambiant. Après un délai de trois secondes, le navigateur et l'application Android arrêtent les enregistrements. le navigateur chiffre ses données et les envoie au serveur, tandis que le téléphone stocke localement les données BLE et audio collectées dans l'application android. La communication entre l'application mobile et le serveur est sécurisée à l'aide du protocole `TLS`.

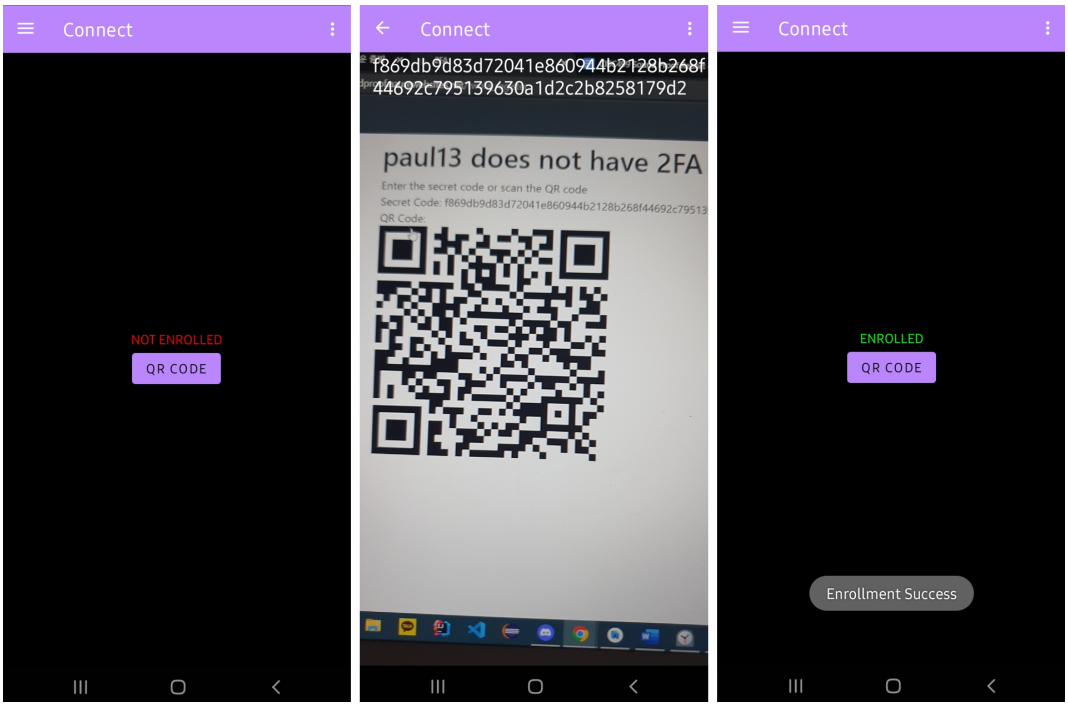


FIGURE 4.10 : Enrollement de l'utilisateur.

4.2.5 ENREGISTREMENT DES SIGNAUX BLE ET DU SON AMBIANT

Dans le navigateur, l'accès au microphone local est obtenu via l'API `navigator.getUserMedia`. De même, l'accès au Bluetooth est géré au niveau du système d'exploitation à l'aide de l'API `BleakScanner.discover()` en `Python`. Nous utilisons des navigateurs populaires tels que *Google Chrome*, *Mozilla Firefox*, *Microsoft Edge*, *Safari* et *Opera*, qui prennent tous en charge l'API `getUserMedia`.

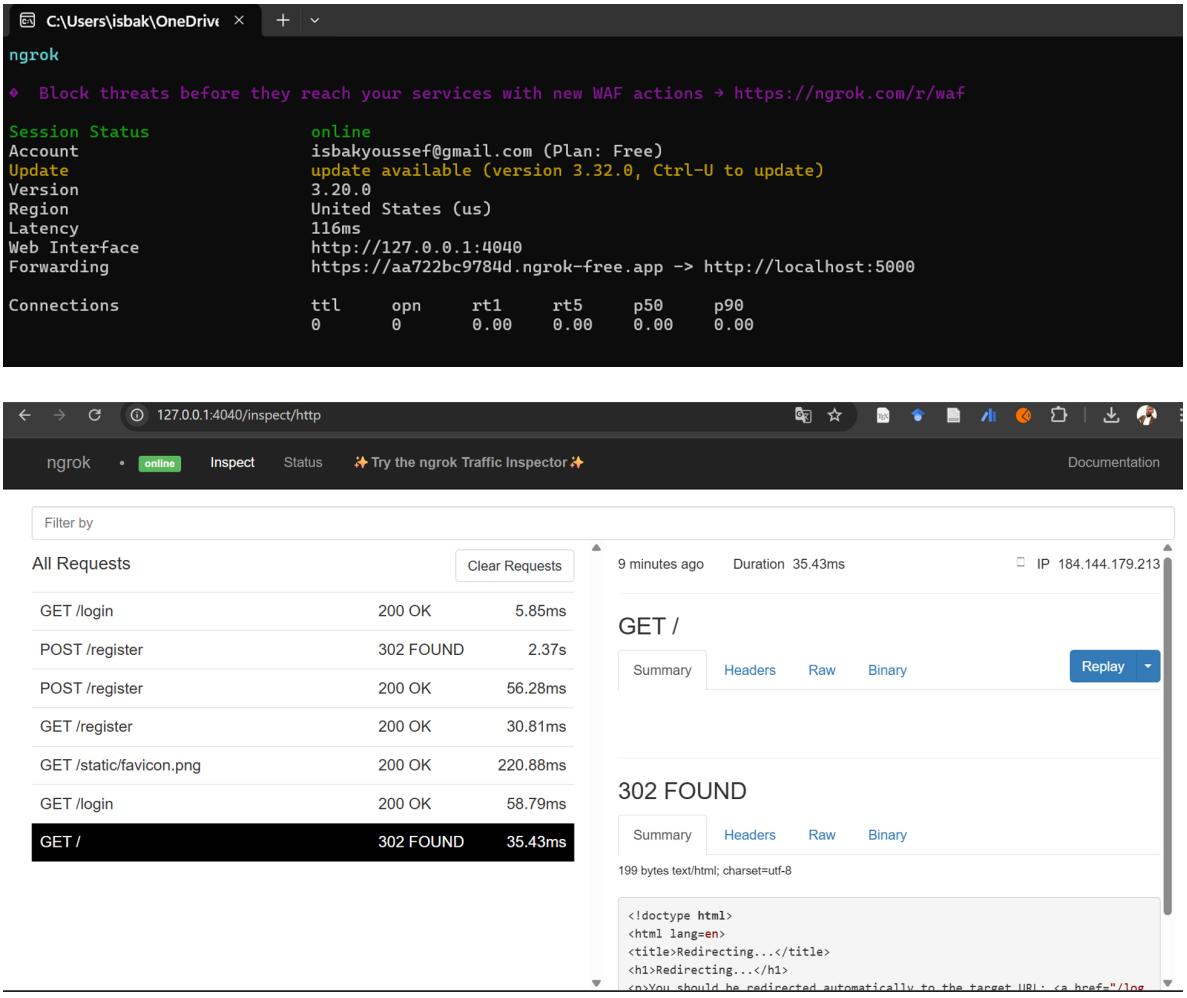


FIGURE 4.11 : Lancement et interface de ngrok.

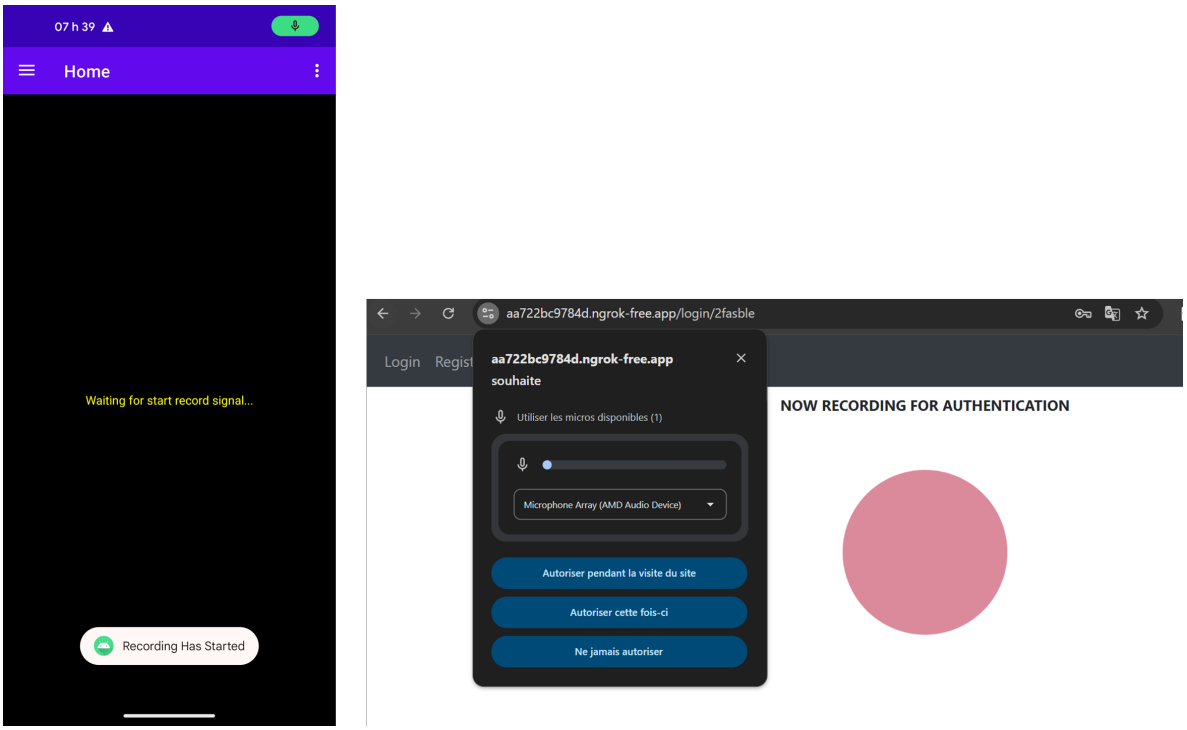


FIGURE 4.12 : Démarrage d'enregistrement côté web et mobile.

Les enregistrements audio et les signaux BLE sont chiffrés à l'aide de l'algorithme `AES-256`, avec une clé symétrique générée pour chaque session. Cette clé est ensuite chiffrée avec la clé publique du téléphone à l'aide du protocole `RSA-2048`. Nos expériences montrent que le système est compatible avec l'ensemble des navigateurs mentionnés. Les enregistrements audio sont envoyés du navigateur vers le serveur via une `API REST Flask`. Grâce à cette API, aucune modification du navigateur ni installation de plug-in n'est nécessaire.

Comme les horloges locales du navigateur et du smartphone peuvent différer, notre implémentation requiert une synchronisation des enregistrements entre les deux appareils. Pour cette raison, les deux dispositifs exécutent un protocole de synchronisation temporelle simple avec le serveur Web. Ce protocole, implémenté sur `HTTP`, permet à chaque appareil de calculer la différence temporelle (θ) entre son horloge locale et celle du serveur. Chaque appareil exécute le protocole de synchronisation avec le serveur pendant l'enregistrement via

son microphone et son capteur Bluetooth. Une fois l'enregistrement terminé, chaque appareil ajuste les horodatages de ses échantillons en fonction de la différence temporelle (θ) calculée par rapport à l'horloge du serveur.

4.2.6 ANALYSE DES SIGNAUX BLE ET AUDIO

Afin de vérifier la proximité physique (ou *co-localisation*) entre les deux dispositifs (ordinateur portable et smartphone), l'application mobile SBLE calcule plusieurs scores de similarité à partir des sons ambiants et des signaux BLE enregistrés.

— Le **score de similarité audio** (S_a), décrit dans la Section 3.3.1, est obtenu en appliquant une banque de filtres passe-bande aux signaux audio afin d'en extraire les composantes dans les bandes d'un tiers d'octave. Pour chaque bande, la corrélation croisée maximale entre les deux signaux est calculée, et la moyenne de ces corrélations constitue la valeur de S_a.

— Le **score de similarité des adresses BLE** (S_j), décrit dans la Section 3.3.2, est mesuré à l'aide de l'indice de Jaccard. Il reflète la proportion d'adresses `BD_ADDR` détectées en commun par les deux dispositifs au cours d'une même fenêtre temporelle.

— Le **score de similarité de la puissance des signaux BLE** (S_r), également décrit dans la Section 3.3.2, est obtenu en calculant la corrélation croisée maximale entre les séries temporelles des valeurs RSSI des adresses BLE détectées par les deux appareils.

Lors du calcul de ces scores de similarité, un décalage temporel maximal de $\ell_{\max} = 150\,\text{ms}$ est toléré, ce qui correspond à la plus grande désynchronisation d'horloge observée au cours de nos expériences.

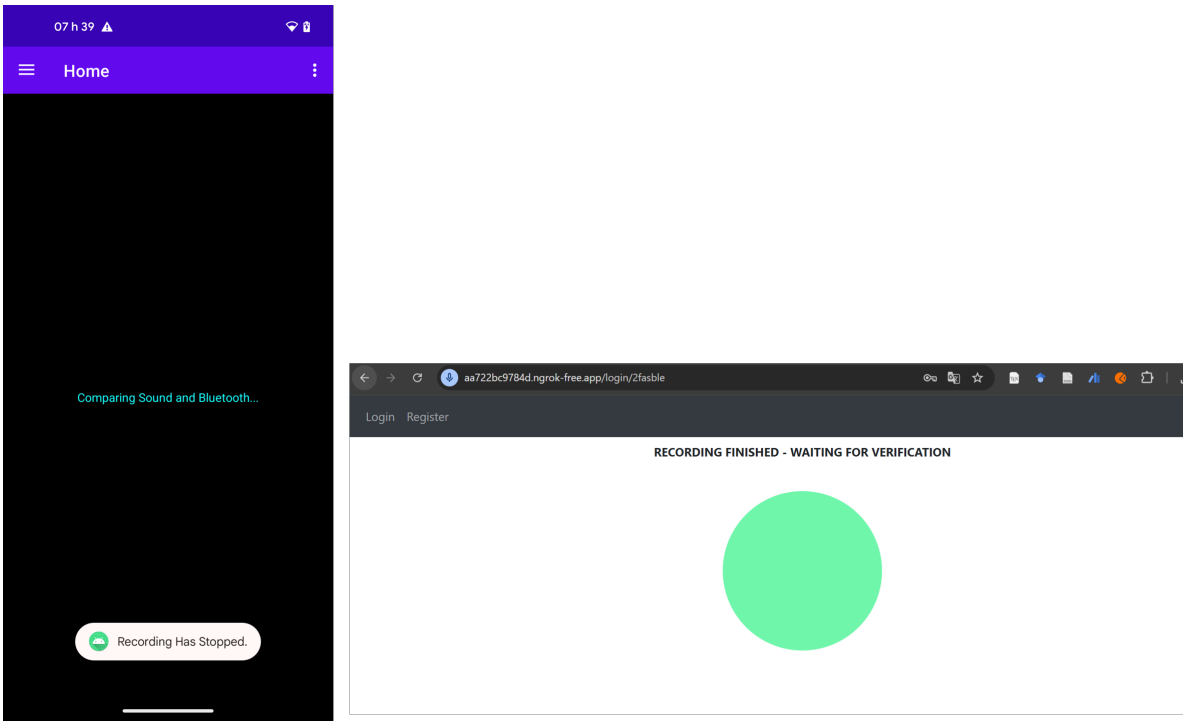


FIGURE 4.13 : Début de calculs des scores de similarités sur l'appareil mobile.

Ces trois scores sont ensuite comparés à des seuils empiriquement déterminés, notés τ_a, τ_j et τ_r, établis expérimentalement afin de distinguer les scénarios de co-localisation effective. L'authentification n'est accordée que si la condition suivante est satisfaite :

$$S_a \geq \tau_a \wedge S_j \geq \tau_j \wedge S_r \geq \tau_r$$

En d'autres termes, les deux dispositifs sont considérés comme co-localisés, et l'authentification est acceptée uniquement si le son ambiant, les adresses BLE détectées et la puissance des signaux BLE présentent un niveau de similarité suffisant.

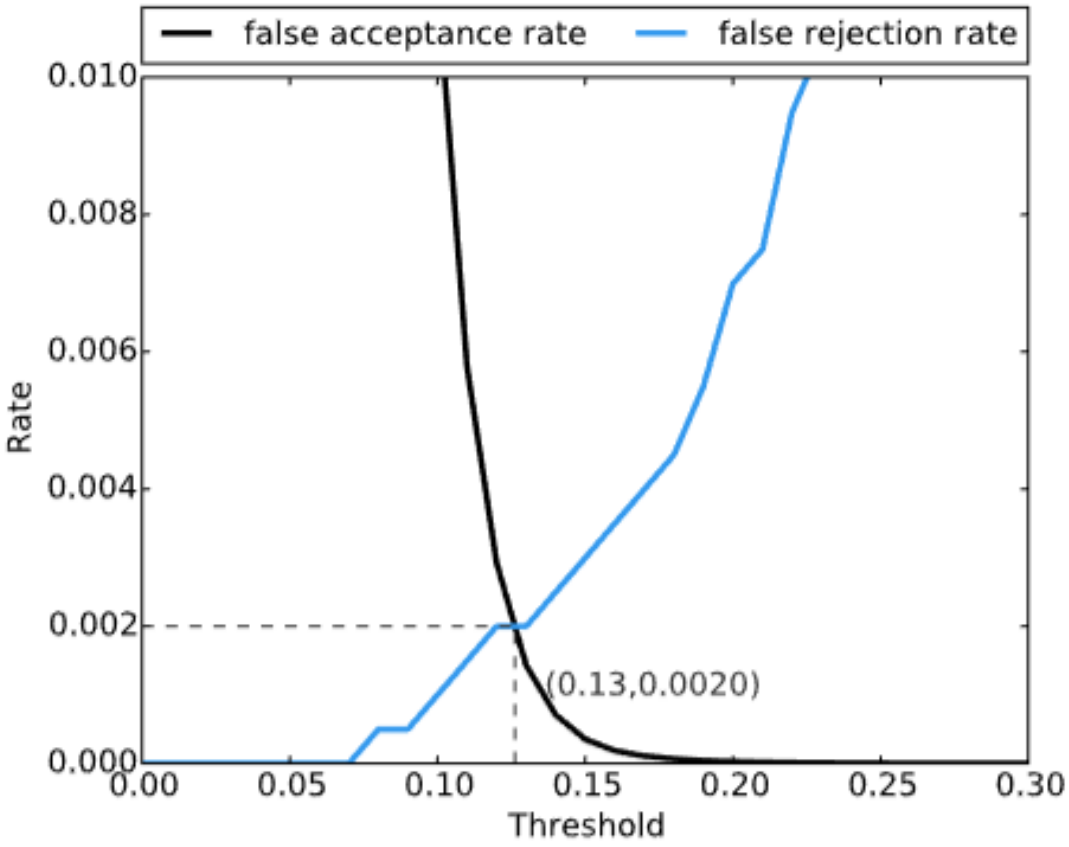


FIGURE 4.14 : Taux de faux rejet (FRR) et taux de fausse acceptation (FAR) en fonction du seuil τ_C pour $B = [50\,\text{Hz} - 4\,\text{kHz}]$. Le taux d'erreur égal (Equal Error Rate, ERR) est de 0.0020 **pour** $\tau_C = 0.13$**.**

Karapanos *et al.* (2015)

Nous avons utilisé un seuil de 0.13 pour les signaux audio, identique à celui employé dans l'étude *Sound-Proof* Karapanos *et al.* (2015). En résumé, les seuils empiriques suivants ont été considérés : $\tau_a = 0.13$, $\tau_j = 0.35$, $\tau_r = 0.2$.

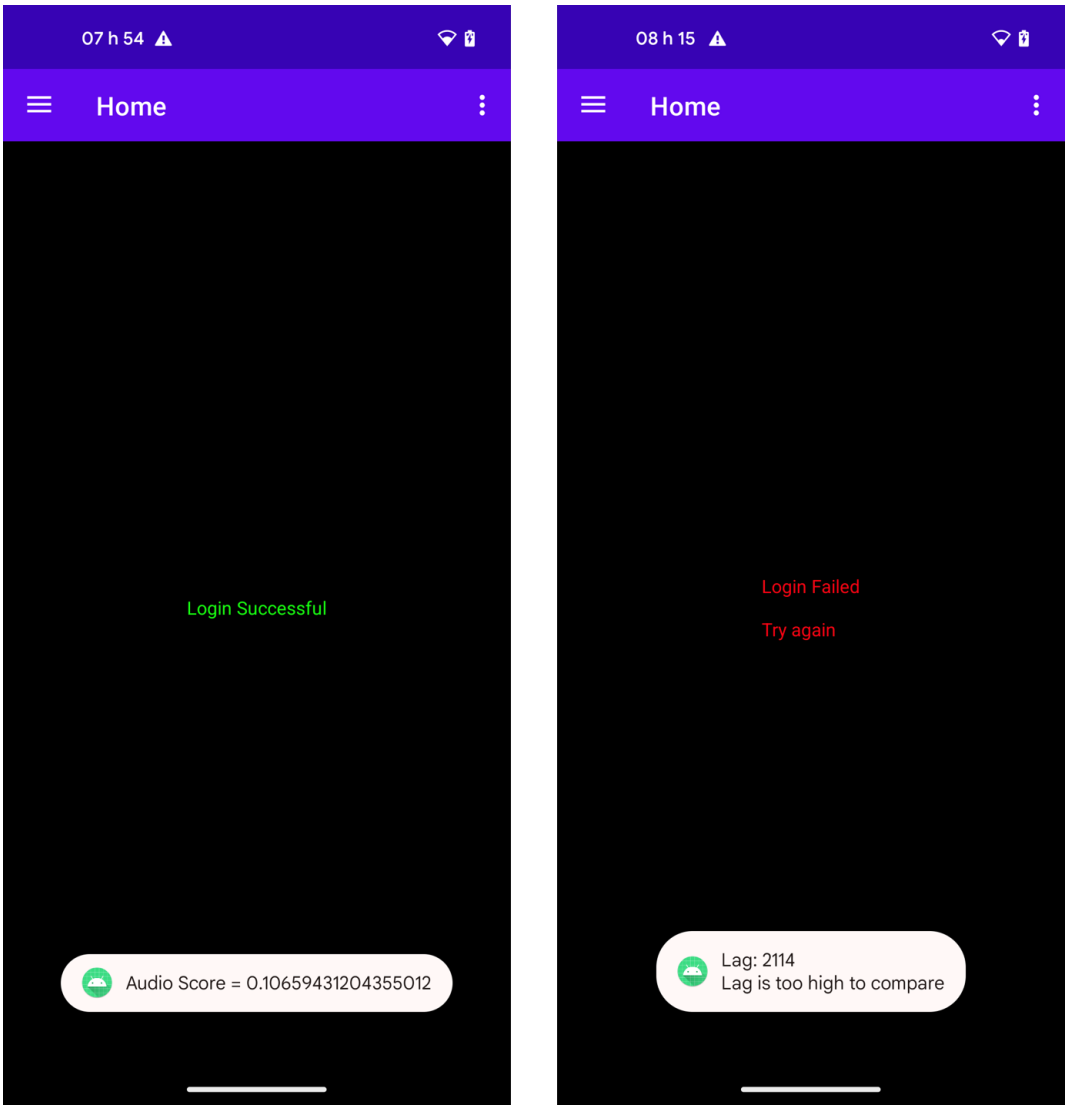


FIGURE 4.15 : Authentification réussie ou réfusée.

Si Login Successful, l'application mobile envoie, un réponse valide au serveur qui à son tour déverouille la session, en donnant l'accès à l'utilisateur. Dans le cas contraire, la session reste vérrouiller et l'utilisateur est appellé à se reconnecter une seconde fois.

CHAPITRE V

ÉVALUATION EXPÉRIMENTALE ET ANALYSE DES RÉSULTATS

Ce chapitre expose la méthodologie expérimentale mise en œuvre pour évaluer SBLE. Les campagnes de tests ont été réalisées dans différents environnements et selon plusieurs conditions d'usage. Les résultats sont analysés à partir de métriques telles que le FAR, le FRR et la précision (Accuracy), puis comparés à ceux de Sound-Proof afin d'évaluer la performance et la robustesse de SBLE.

5.1 ÉVALUATION

Dans cette partie, nous évaluons principalement le système *SBLE* dans des scénarios où des attaquants coexistent avec l'utilisateur légitime. En effet, *SBLE* offre une forte protection contre les attaquants distants grâce à sa nature hybride. Pour atteindre leur objectif, les attaquants devraient manipuler non seulement les données audio ambiantes, mais aussi les signaux BLE, ce qui est extrêmement difficile puisque les signaux sans fil environnementaux sont fortement sensibles à la position, c'est-à-dire que leurs caractéristiques varient selon la localisation spatiale.

De plus, nous réalisons une analyse d'utilisabilité et de sécurité du système *SBLE* et le comparons avec les schémas classiques d'authentification à deux facteurs sans effort tels que *Sound-Proof* Karapanos *et al.* (2015).

5.1.1 CONFIGURATION EXPÉRIMENTALE

Nous avons déployé un serveur pour héberger notre prototype et collecter des paires d'échantillons à partir de requêtes de connexion initiées depuis des navigateurs. Trois participants ont été impliqués, utilisant des :

- ordinateurs portables : HP Ryzen 7 sous Windows 11, Lenovo i7 sous Windows 11
- ordinateurs de bureau : HP i7 sous Windows 10.
- smartphones : Samsung Galaxy S9+ sous android 14, Google Pixel 5 sous Android 14.

Les connexions ont été effectuées à l'aide des navigateurs Google Chrome, Microsoft Edge, Firefox et Safari sur une période de six semaines.

FIGURE 5.1 : Les navigateurs web utilisés

Pour chaque tentative de connexion, le smartphone de l'utilisateur et le navigateur ont enregistré simultanément les sons ambiants via leurs microphones et les signaux Bluetooth via leurs modules BLE pendant une durée de trois (3) secondes.

Une tentative de connexion était considérée comme légitime lorsqu'elle était initiée à moins de 1.5 m du téléphone enregistré et présentait une cohérence temporelle. Dans le cas contraire, elle était traitée comme une tentative d'attaque.

Les expériences ont été menées dans trois environnements représentatifs :

- **Bureau** : un environnement relativement calme avec des bruits de fond modérés, tels que la frappe au clavier ;
- **Café** : un environnement semi-bruyant caractérisé par des conversations animées et de la musique d'ambiance ;
- **Domicile** : un environnement domestique avec un bruit de fond modéré, principalement issu des sons de la télévision.

Nous avons collecté un total de 871 tentatives de connexion, correspondant à 871 échantillons audio et 871 échantillons BLE. Pour chaque tentative, nous avons calculé :

- la similarité temporelle et fréquentielle des signaux audio ;
- la similarité structurelle entre les ensembles d'adresses BLE ;
- la similarité des puissances de signaux BLE (RSSI) entre le téléphone et l'ordinateur correspondant.

Parmi l'ensemble des données collectées, 342 paires d'échantillons provenaient d'utilisateurs légitimes, tandis que 529 paires provenaient d'attaquants co-localisés.

5.1.2 PRÉTRAITEMENT DES DONNÉES

Avant toute comparaison, les données collectées ont été soumises à une phase de prétraitement visant à réduire le bruit et à normaliser les signaux.

Audio : De manière similaire à *Sound-Proof* Karapanos *et al.* (2015), nous avons appliqué un filtrage en bandes d'octaves tiers (*one-third octave bands*) pour décomposer les enregistrements audio de 3 secondes en 20 bandes couvrant la plage $B = [50\,\text{Hz}, 4\,\text{kHz}]$. Cette approche permet d'extraire les composantes fréquentielles représentatives. Les amplitudes ont ensuite été normalisées, et un seuillage du spectrogramme a été appliqué afin d'atténuer l'impact du bruit de fond. De plus, un seuil de puissance moyenne de $\tau_{dB} = 40\,\text{dB}$ a été fixé pour éliminer automatiquement les enregistrements silencieux ou de faible intensité.

Signaux BLE : Les trames ayant une valeur RSSI inférieure à $-75\,\text{dBm}$ ont été supprimées en raison de leur faible pouvoir discriminant entre utilisateurs légitimes et attaquants co-localisés. Les adresses `BD_ADDR` détectées ont été extraites et associées à leurs valeurs RSSI correspondantes. Les données ont ensuite été agrégées dans des fenêtres temporelles fixes, et les doublons supprimés afin de construire un ensemble d'échantillons représentatif et non redondant.

Synchronisation Temporelle : La synchronisation entre le smartphone et l'ordinateur a été maintenue avec une tolérance de $\ell_{\max} = 150\,\text{ms}$, garantissant la comparabilité des signaux collectés dans des conditions réalistes.

5.2 MÉTRIQUES DE PERFORMANCE

Pour l'évaluation, nous avons utilisé une matrice de confusion 2×2 contenant le nombre de *vrais positifs* (TP), *faux négatifs* (FN), *faux positifs* (FP) et *vrais négatifs* (TN), afin d'indiquer les performances du système *SBLE*.

À partir de ces valeurs, nous définissons plusieurs métriques permettant d'évaluer les performances globales de *Sound-Proof* et de notre système proposé *SBLE*, puis nous comparons leurs résultats. Parmi les plus couramment utilisées figurent le FRR, le FAR, l'exactitude (accuracy), la précision (precision), le rappel (recall) et le F1-score.

- **Taux de faux rejet** (FRR) : Il mesure la proportion de tentatives d'authentification légitimes (réelles) qui sont rejetées à tort par le système. Autrement dit, c'est la probabilité qu'un utilisateur légitime soit refusé par erreur. Un FRR faible signifie que le système est confortable et pratique à utiliser (bonne expérience utilisateur). Un FRR élevé indique que le système rejette trop souvent des utilisateurs valides, ce qui nuit à la convivialité du mécanisme d'authentification.

$$FRR = \frac{FN}{FN + TP}$$

- **Taux de fausse acceptation** (FRR) : Il correspond à la proportion de tentatives d'authentification frauduleuses (attaques) qui sont incorrectement acceptées par le système comme étant légitimes. Autrement dit, c'est la probabilité qu'un attaquant soit authentifié par erreur.

$$FAR = \frac{FP}{TP + FP}$$

- **Exactitude (Accuracy)** : L'Accuracy mesure la proportion totale de prédictions correctes (autant positives que négatives) parmi toutes les prédictions effectuées par le système. Autrement dit, c'est la probabilité qu'une décision soit correcte, qu'il s'agisse d'une acceptation ou d'un rejet. Une accuracy élevée indique que le système prend globalement de bonnes décisions. Cependant, elle peut être trompeuse si les classes sont déséquilibrées (ex. beaucoup plus de connexions légitimes que d'attaques)

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

- **Précision (Precision)** : La précision mesure la proportion des cas identifiés comme positifs qui sont réellement positifs. Autrement dit, elle indique la fiabilité des détections positives du système. Une précision élevée signifie que la majorité des authentifications acceptées sont effectivement légitimes.

$$Precision = \frac{TP}{TP + FP}$$

- **Rappel (Recall)** : Le rappel indique la proportion des vrais positifs parmi tous les éléments qui auraient dû être détectés comme positifs. Un rappel élevé signifie que le système rate peu de cas positifs (peu de faux négatifs). Dans le contexte d'un système d'authentification comme SBLE, cela veut dire :peu de rejets erronés d'utilisateurs légitimes, donc une meilleure expérience utilisateurCette métrique est cruciale dans des contextes dans lesquels il est essentiel de minimiser les faux négatifs.

$$Recall = \frac{TP}{TP + FN}$$

- **F1-Score** : Elle combine la précision et le rappel en une métrique harmonisée, offrant un équilibre entre les deux. elle est une métrique qui combine la précision et le rappel en une seule valeur pour évaluer la performance globale d'un système de classification ou d'authentification. Elle exprime un équilibre entre la capacité du système à bien détecter les vrais utilisateurs (rappel) et à éviter les fausses acceptations (précision).

$$F1\text{-}Score = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

où

— TP (Vrai Positif) tentatives légitimes acceptées,

— TN (Vrai Négatif) attaques correctement rejetées.

— FP (Faux Positif) attaques acceptées à tort,

— FN (Faux Négatif) tentatives légitimes rejetées à tort,

5.3 ANALYSE DES RÉSULTATS DE L'ÉVALUATION

Nous menons des expériences pour évaluer SBLE dans les trois environnements mentionnés ci-dessus 5.1.1 ; nous considerons deux positions de smartphone de l'utilisateur qui sont :

— sur la table du bureau ;

— dans la poche de l'utilisateur ;

Dans cette partie, nous présentons les résultats de l'évaluation de notre système, en mettant l'accent sur son utilité et sa sécurité. Le protocole d'évaluation suit la méthodologie proposée dans les travaux de *Sound-Proof* Karapanos *et al.* (2015) et He *et al.* (2022)

5.3.1 ÉVALUATION DE L'UTILITÉ

Afin de démontrer que notre système SBLE offre une bonne expérience utilisateur, nous avons mesuré le FRR, c'est-à-dire la probabilité qu'une tentative d'accès légitime effectuée par un utilisateur autorisé soit incorrectement rejetée par le système.

Environnement de bureau

Lorsque le smartphone est sur la table, le nombre total de tentatives de connexion est de 50 et le nombre de tentatives rejetées à tort du schéma Sound-Proof est de 7, tandis que celui du schéma SBLE est de 2 ; lorsque le smartphone est dans une poche, le nombre total de tentatives de connexion est de 49 et le nombre de tentatives rejetées à tort du schéma Sound-Proof est de 22, tandis que celui du schéma SBLE est de 4.

Environnement domicile

Lorsque le téléphone est sur la table, le nombre total de tentatives de connexion est de 62 et le nombre de tentatives rejetées à tort des schémas Sound-Proof et SBLE est de 0 ; Lorsque le téléphone est dans la poche, le nombre total de tentatives de connexion est de 60 et le nombre de tentatives incorrectement rejetées du schéma Sound-Proof et du schéma SBLE est de 1.

Environnement de Café

Lorsque le téléphone est sur la table, le nombre total de tentatives de connexion est de 67 et le nombre de tentatives incorrectement rejetées du schéma Sound-Proof du schema SBLE est de 1 ; lorsque le smartphone est dans une poche, le nombre total de tentatives de connexion est de 54 et le nombre de tentatives incorrectement rejetées du schéma Sound-Proof est de 6, tandis que celui du schéma SBLE est de 3.

TABLEAU 5.1 : FRR dans différents environnements

Position	Système	Bureau	Café	Domicile
Sur le bureau	Sound-Proof	0.14	0	0.0167
	SBLE	0.04	0	0
Dans la poche	Sound-Proof	0.4489	0.0167	0.1111
	SBLE	0.0816	0.0167	0.0555

Le Tableau 5.1 présente le FRR mesuré pour chaque environnement et chaque modalité de placement.

Les résultats montrent que le FRR de SBLE reste inférieur à 9% dans toutes les conditions, avec une moyenne globale de 3.22%. Le FRR est légèrement plus élevé lorsque le téléphone est dans la poche, en raison de l'atténuation des signaux sonores. Toutefois, ce taux reste acceptable pour un usage pratique d'authentification à deux facteurs zéro-effort et continue, en comparaison avec *Sound-Proof* dont le FRR dépassait 44% dans certains cas.

5.3.2 ÉVALUATION DE LA SÉCURITÉ

Un système est considéré comme non sécurisé lorsqu'un adversaire proche ou distant parvient à passer l'authentification. Nous mesurons la sécurité de notre système d'authentification à l'aide du FAR, qui représente la probabilité que le système accepte à tort la tentative d'accès d'un utilisateur non autorisé.

Dans ce qui suit, nous avons mis en place deux types de situations d'attaque pour mener des attaques relativement proches et des attaques relativement éloignées. Dans le premier cas,

l'attaquant se trouve à environ 1,5 m à 5 m de la victime (appelé « relativement proche »). Dans le second cas, ils sont séparés de 7 m ou plus (appelé « relativement éloigné »).

Environnement de bureau

Lorsque le téléphone est placé sur la table, nous avons enregistré 55 tentatives d'attaque relativement proches et 46 tentatives relativement éloignées. Pour le schéma Sound-Proof, 24 attaques proches et 11 attaques éloignées ont été acceptées. En revanche, pour le schéma SBLE, seules 3 attaques proches ont été acceptées et 1 attaque éloignée a été acceptée. Lorsque le téléphone est placé dans une poche, nous avons enregistré 43 tentatives proches et 37 tentatives éloignées. Avec le schéma Sound-Proof, 12 attaques proches et 8 attaques éloignées ont été acceptées. Pour le schéma SBLE, une seule attaque proche a été acceptée et aucune attaque éloignée n'a abouti.

Environnement de Café

Lorsque le téléphone est placé sur la table, nous avons enregistré 63 tentatives proches et 51 tentatives éloignées. Pour le schéma Sound-Proof, 26 attaques proches et 11 attaques éloignées ont été acceptées. Quant au schéma SBLE, seules 4 attaques proches ont été acceptées et 1 attaque éloignée a été acceptée . Lorsque le téléphone est placé dans une poche, nous avons enregistré 41 tentatives proches et 33 tentatives éloignées. Avec le schéma Sound-Proof, 11 attaques proches et 6 attaques éloignées ont été acceptées. Pour le schéma SBLE, 2 attaques proches et 1 attaque éloignée ont été acceptées.

Environnement Domicile

Lorsque le téléphone est placé sur la table, nous avons enregistré 48 tentatives proches et 43 tentatives éloignées. Pour le schéma Sound-Proof,21 attaques proches et 9 attaques éloignées ont été acceptées. Du côté du schéma SBLE, 4 attaques proches et 2 attaques

éloignées ont été acceptées. Lorsque le téléphone est placé dans une poche, nous avons enregistré 37 tentatives proches et 32 tentatives éloignées. Avec le schéma Sound-Proof, 11 attaques proches et 7 attaques éloignées ont été acceptées. En revanche, pour le schéma SBLE, seules 3 attaques proches et aucune attaque éloignée n'a abouti.

Le Tableau 5.2 présente le FAR mesuré dans différents environnements et scénarios.

TABLEAU 5.2 : FAR dans différents environnements

Position	Type d'attaque	Système	Bureau	Café	Domicile
Sur le bureau	Relativement proche	Sound-Proof	0.4363	0.4126	0.4375
		SBLE	0.0545	0.0635	0.0833
	Relativement éloignée	Sound-Proof	0.2391	0.2156	0.2093
		SBLE	0.0217	0.0196	0.0465
Dans la poche	Relativement proche	Sound-Proof	0.2791	0.2683	0.2973
		SBLE	0.0232	0.0487	0.0811
	Relativement éloignée	Sound-Proof	0.2162	0.1818	0.2187
		SBLE	0	0.0303	0

Les résultats indiquent que SBLE maintient un FAR extrêmement bas, inférieur à 9% dans tous les cas, ce qui démontre la robustesse de la combinaison Audio + BLE. Comparé à *Sound-Proof* dont le FAR pouvait dépasser 43% en environnement musical, SBLE offre une nette amélioration.

5.3.3 MÉTRIQUES DE PERFORMANCE GLOBALES

Ces résultats montrent que SBLE atteint un équilibre robuste entre utilité et sécurité, avec une haute précision globale et un faible taux de faux positifs.

TABLEAU 5.3 : Résultats globaux des performances de SBLE

Métrique	Valeur
FAR	3,22 %
FRR	4,16 %
Précision	94,03 %
F-mesure	95,40 %

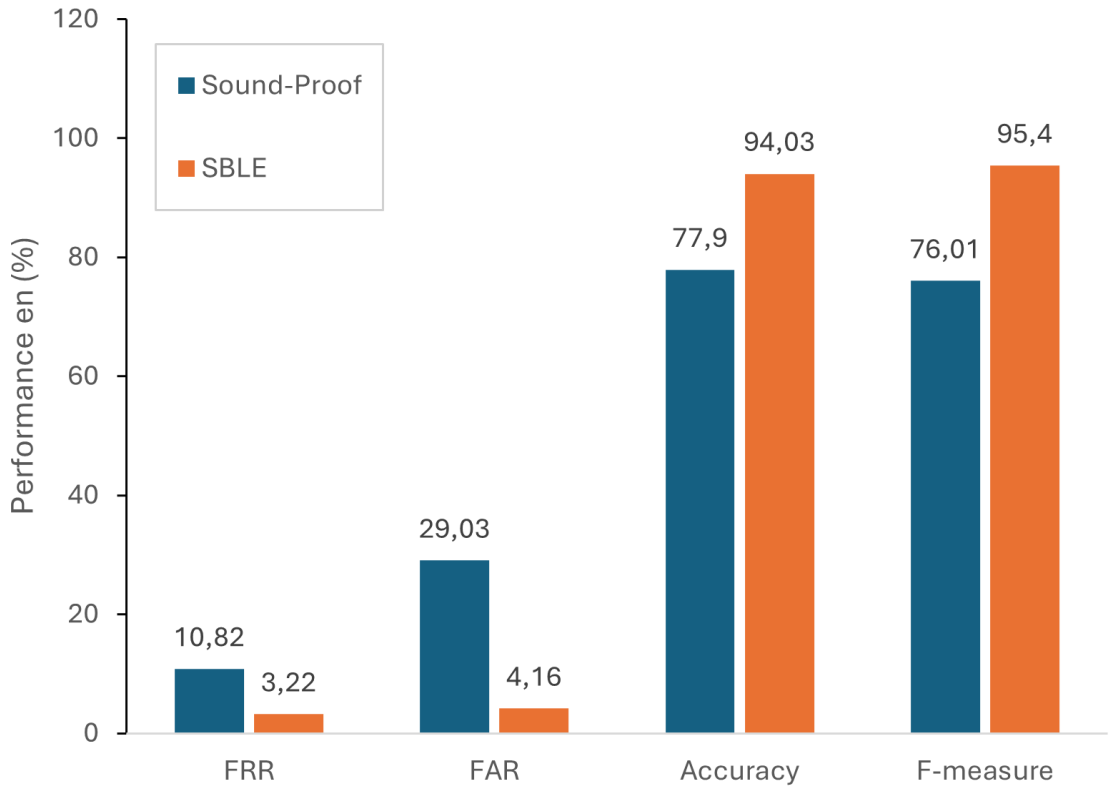


FIGURE 5.2 : SBLE versus Sound-Proof Performances

En résumé, nous avons évalué SBLE dans deux environnements de travail représentatifs, en présence d'adversaires, et obtenu une précision moyenne de 94,03%. Ce résultat est jugé acceptable en l'absence d'interaction directe entre l'utilisateur et son téléphone. De plus, nous n'avons pas effectué d'attaques à distance qui seraient théoriquement détectables par SBLE.

Cette précision élevée associée à un faible taux de fausses acceptations indique la fiabilité de SBLE dans différentes situations.

CHAPITRE VI

DISCUSSION ET LIMITES

Dans ce chapitre, nous discutons des apports et les limites de SBLE, en soulignant les avantages de son approche hybride et les défis rencontrés lors de sa mise en œuvre. Il propose également des perspectives d'amélioration, notamment l'intégration de nouveaux paramètres contextuels et l'optimisation du processus de décision. Enfin, il conclut sur les contributions majeures de cette recherche et sur les enseignements tirés de l'évaluation expérimentale.

6.1 EXIGENCES LOGICIELLES ET MATÉRIELLES

Comme tout autre mécanisme d'authentification à deux facteurs (2FA) basé sur des jetons logiciels Karapanos *et al.* (2015), SBLE nécessite une application installée sur le téléphone de l'utilisateur.

Cependant, SBLE ne requiert aucun logiciel supplémentaire sur l'ordinateur et fonctionne de manière transparente avec tout navigateur compatible HTML5 implémentant l'API WebRTC. Les navigateurs tels que Google Chrome, Firefox, Opera et Internet Explorer, Microsoft Edge prennent tous en charge WebRTC. De plus, SBLE nécessite que le téléphone dispose d'une connexion Internet. Le téléphone et l'ordinateur sur lequel le navigateur est exécuté doivent tous deux être équipés d'un microphone et de capteurs Bluetooth Low Energy (BLE). Ces composants sont omniprésents sur les téléphones, tablettes et ordinateurs portables.

Si un ordinateur, tel qu'un PC de bureau, ne possède pas de microphone intégré, SBLE nécessitera l'utilisation d'un microphone externe, par exemple celui intégré à une webcam.

6.2 CONFIDENTIALITÉ

L'environnement sonore ambiant ainsi que les données BLE de l'utilisateur peuvent potentiellement révéler des informations privées à un serveur malveillant.

Dans notre conception, et afin d'assurer une meilleure protection de la vie privée, le serveur est modélisé comme une menace potentielle. Il doit transmettre la clé publique du téléphone (pk) à l'ordinateur client lors de la réception d'une requête de connexion. Ensuite, le navigateur chiffre ses échantillons audio et BLE à l'aide de pk, puis les envoie au téléphone en utilisant le serveur comme proxy. À la réception des textes chiffrés transmis par le serveur, le téléphone les déchiffre à l'aide de sa clé privée sk.

Cependant, un serveur malveillant peut également tenter d'accéder au microphone et au capteur BLE de l'ordinateur lorsque l'utilisateur visite la page web de ce serveur.

En pratique, tous les navigateurs que nous avons testés demandent une autorisation explicite de l'utilisateur avant d'activer l'accès au microphone ou au Bluetooth via la fonction `getUserMedia`. De plus, les navigateurs affichent une alerte lorsqu'un site web déclenche un enregistrement audio. Les adresses `BD_ADDR` et les mesures `RSSI` restent des informations publiques et non sensibles.

6.3 ENVIRONNEMENTS SILENCIEUX ET ABSENCE DE SIGNAUX BLUETOOTH DÉTECTABLES

Sound-Proof rejette une tentative de connexion si la puissance de l'un des échantillons audio est inférieure à τ_{dB}. Dans le cas où l'environnement est trop silencieux, le site web peut inviter l'utilisateur à produire un bruit quelconque (par exemple, en se raclant la gorge, en tapant sur la table, etc).

SBLE vient éviter cette tâche a l'utilisateur car dans un environnement silencieux, car il fonctionne correctement en se basant que sur les données BLE dans ce type d'environnement, de même dans un environnement où il ya une fluctuation des signaux BLE ou quasiment pas de signaux BLE detectables, les données audios prennent le relais ce qui le rend plus robuste.

6.4 AUTHENTIFICATION CONTINUE

SBLE intègre un mécanisme d'authentification continue, implémenté à travers un algorithme développé et traduit en Python. Cet algorithme reproduit le comportement du système réel en surveillant en permanence l'environnement de l'utilisateur. Cette fonctionnalité collecte périodiquement de nouvelles données issues des signaux BLE et de l'audio ambiant au moyen d'une boucle de contrôle. Si les enregistrements provenant des deux appareils ne correspondent plus, le serveur peut alors forcer la déconnexion de l'utilisateur afin de prévenir tout accès non autorisé.

Toutefois, cette approche présente un inconvénient notable : elle entraîne une consommation énergétique accrue, pouvant affecter l'autonomie de la batterie du smartphone

6.5 ÉCHECS DE CONNEXION ET LIMITATION DES TENTATIVES

SBLE considère une tentative de connexion comme frauduleuse si les scores de similarités (respectivement le score de similarité audio et le score de similarité BLE) entre les deux échantillons de deux types de données sont inférieurs respectivement au seuil τ_a, τ_j et τ_r.

Dans ce cas, le serveur demande aux deux appareils de répéter l'enregistrement et la comparaison. Après 3 échecs, le serveur peut passer à une authentification basée sur un code de vérification. Ce qui évite les attaques par force brute et préserve l'autonomie de la batterie du téléphone.

6.6 ANALYSE DE SÉCURITÉ

Attaques à distance

Les adversaires distants ne peuvent pas déterminer avec précision le moment où le téléphone de l'utilisateur commence à enregistrer le signal, puisque ce mécanisme est déclenché par l'ordinateur local. Leur seule possibilité repose sur une éventuelle collision obtenue après de multiples tentatives de connexion. Cependant, même dans ce cas, ils ne peuvent pas lancer d'attaque réussie contre SBLE.

Il est envisageable que certains adversaires tentent des attaques par prédiction sonore, puisque SBLE exploite l'environnement sonore ambiant pour établir la colocalisation. Toutefois, une telle attaque ne pourrait être valide que si l'attaquant parvient à prédire simultanément l'environnement sonore ambiant et l'environnement BLE dynamique de l'utilisateur.

En pratique, cela s'avère hautement improbable : sans disposer d'informations de localisation précises ou du numéro de téléphone de la victime (à partir duquel l'attaquant pourrait tenter de faire sonner le téléphone), il est impossible d'anticiper ou de reproduire fidèlement le contexte réel de l'utilisateur.

Même des adversaires puissants, capables de détecter les appareils sans fil environnants grâce à la localisation ou capable d'avoir le numéro de téléphone de la victime, restent confrontés à des limitations majeures. En effet, la prédiction et la simulation d'un environnement BLE identique sont rendues difficiles par le caractère aléatoire des adresses `BD_ADDR` et la variabilité instantanée des mesures `RSSI`. De plus, le téléphone de l'utilisateur peut être en mode silencieux, ce qui peut réduire considérablement les chances de réussir une attaque par prédiction sonore.

Ainsi, dans SBLE, de tels adversaires ne peuvent en aucun cas être considérés comme des utilisateurs légitimes.

Attaques de coexistence

Les adversaires coexistants sont plus proches de l'utilisateur légitime et plus susceptibles d'obtenir un contexte similaire. Cependant, SBLE peut efficacement résister à de tels comportements.

SBLE exploite les signaux BLE environnementaux et les signaux audios ambiants sensibles à la localisation pour faciliter la détection de colocalisation. Ainsi, même si ces adversaires coexistent avec l'utilisateur, il pourrait obtenir des données audios similaires mais difficilement des données BLE très similaires. Les résultats de l'évaluation montrent une précision de 94,04%. Cela signifie que la plupart des adversaires coexistants ont été identifiés avec précision.

6.7 CONTRIBUTION

Ce travail apporte une contribution majeure à la conception d'un schéma d'authentification à deux facteurs (2FA) sans effort, continu, robuste et adaptable, à travers la proposition de SBLE, un système hybride combinant les signaux Bluetooth Low Energy (BLE) et audio ambiants pour une détection fiable de la co-localisation entre les appareils d'un utilisateur.

En s'appuyant sur les limites observées dans les systèmes Sound-Proof Karapanos *et al.* (2015), vulnérables aux attaques par relecture ou par prédiction sonore et inefficaces dans les environnements silencieux, ainsi que dans ABLE He *et al.* (2022), dont les performances dépendent fortement de la densité des appareils à proximité, SBLE surmonte leurs faiblesses respectives en intégrant deux modalités complémentaires : les signaux audio, efficaces dans

les environnements riches en sons, et les signaux BLE, plus stables dans les environnements calmes ou densément peuplés d'appareils BLE.

Cette fusion multimodale permet à SBLE d'offrir une authentification à deux facteurs continue et sans interaction utilisateur, en vérifiant périodiquement la proximité physique entre le poste de travail et le smartphone. L'algorithme développé, basé sur la corrélation croisée normalisée, l'indice de Jaccard, et l'évaluation combinée des similarités de formes d'onde et d'intensités RSSI, assure une prise de décision fiable tout en minimisant le taux de fausses acceptations.

Le système a été implémenté et évalué expérimentalement dans différents contextes d'utilisation, démontrant une précision moyenne de 94,03% et une résilience élevée face aux attaques à distance et de co-présence, tout en maintenant une expérience utilisateur fluide et transparente.

Enfin, cette recherche, soumise pour évaluation en vue d'une éventuelle publication à la conference ACM, The 16th ACM Conference on Data and Application Security and Privacy (CODASPY), apporte une contribution significative à la modélisation et à l'évaluation des performances des systèmes d'authentification Zero-Effort, en introduisant une approche hybride et multi-sensorielle conciliant sécurité, flexibilité et facilité de déploiement.

CONCLUSION

Dans ce mémoire, nous avons proposé SBLE, un mécanisme 2FA sans effort et continu exploitant la colocalisation des appareils à travers les signaux audio et Bluetooth Low Energy.

L'objectif principal de cette recherche était de concevoir un mécanisme capable d'authentifier un utilisateur en vérifiant la colocalisation entre son smartphone et le terminal de connexion, sans nécessiter d'intervention explicite, tout en réduisant de faux positifs. SBLE repose sur une approche hybride combinant les signaux audio ambiants (riche en variabilité temporelle et spatiale) et les signaux BLE pour déterminer si les deux appareils partagent le même environnement. Cette combinaison permet de compenser les faiblesses individuelles de chaque modalité : BLE et audio.

Sur le plan méthodologique, nous avons conçu une architecture modulaire composée d'un navigateur et d'un smartphone collaborant pour vérifier la proximité réelle de l'utilisateur. Afin de préserver la confidentialité, les données brutes ne sont jamais transmises au serveur : elles sont chiffrées localement à l'aide d'un schéma hybride AES-256/RSA-2048, garantissant ainsi la protection des informations sensibles. La similarité des signaux est ensuite évaluée par des fonctions de corrélation croisée maximale, de normalisation et de l'indice de jaccard, permettant de distinguer les connexions légitimes des tentatives d'authentification frauduleuses.

Les résultats expérimentaux obtenus démontrent que SBLE atteint une meilleure précision globale que Sound-Proof He *et al.* (2022) et ABLE Karapanos *et al.* (2015), tout en conservant une expérience utilisateur fluide. Les mesures de performance (FAR, FRR, accuracy et F-measure) ont confirmé que SBLE réduit significativement les taux de fausse acceptation et de faux rejet. De plus, nos tests en environnements variés (silencieux, modérément bruyants et

dynamiques) ont montré la robustesse du système face aux attaques à distance et aux attaques de co-existence, tout en maintenant des performances stables.

Au-delà de ces résultats prometteurs, SBLE ouvre la voie à plusieurs axes de recherche futurs. D'une part, l'intégration de techniques d'apprentissage automatique pour l'adaptation dynamique des seuils de similarité pourrait améliorer encore la précision du système dans des contextes variés. D'autre part, le déploiement à grande échelle dans des environnements réels (entreprises, systèmes IoT, contrôle d'accès). permettrait de renforcer la robustesse de la détection de co-localisation dans des environnements complexes.

BIBLIOGRAPHIE

Abuhamad, M., Abuhmed, T., Mohaisen, D. & Nyang, D. (2020). AUToSen : Deep-learning-based implicit continuous authentication using smartphone sensors. *IEEE Internet of Things Journal*, *7*(6), 5008–5020.

Acar, A., Aksu, H., Uluagac, A. S. & Akkaya, K. (2020). A usable and robust continuous authentication framework using wearables. *IEEE Transactions on Mobile Computing*, *20*(6), 2140–2153.

Acar, A., Ali, S., Karabina, K., Kaygusuz, C., Aksu, H., Akkaya, K. & Uluagac, S. (2021). A lightweight privacy-aware continuous authentication protocol-PACA. *ACM Transactions on Privacy and Security (TOPS)*, *24*(4), 1–28.

Acar, A., Liu, W., Beyah, R., Akkaya, K. & Uluagac, A. S. (2019). A privacy-preserving multifactor authentication system. *Security and Privacy*, *2*(5), e88.

Agadakos, I., Hallgren, P., Damopoulos, D., Sabelfeld, A. & Portokalidis, G. (2016). Location-enhanced authentication using the IoT : Because you cannot be in two places at once. Dans *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pp. 251–264.

Agrawal, M., Mehrotra, P., Kumar, R. & Shah, R. R. (2022). Gantouch : An attack-resilient framework for touch-based continuous authentication system. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *4*(4), 533–543.

Aksu, H., Uluagac, A. S. & Bentley, E. S. (2018). Identification of wearable devices with bluetooth. *IEEE Transactions on Sustainable Computing*, *6*(2), 221–230.

AlQahtani, A. A. S., Alshayeb, T., Nabil, M. & Patooghy, A. (2024). Leveraging machine learning for wi-fi-based environmental continuous two-factor authentication. *IEEE Access*, *12*, 13277–13289.

AlQahtani, A. A. S., El-Awadi, Z. & Min, M. (2021). A survey on user authentication factors. Dans *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 0323–0328. IEEE.

Atallah, Z., JosephNg, P. & Phan, K. (2021). JomNFC : Zero effort intelligent access system. Dans *2021 Innovations in Power and Advanced Computing Technologies (i-PACT)*, pp. 1–6. IEEE.

Bonnie, E. (2025). *Incident de sécurité dans le monde*. Repéré à https://secureframe.com/blog/data-breach-statistics

Can, Z. & Atılgan, E. (2023). A Review of Recent Machine Learning Approaches for Voice Authentication Systems. *Bilgi ve İletişim Teknolojileri Dergisi*, *5*(1), 96–114.

Cao, Y., Zhang, Q., Li, F., Yang, S. & Wang, Y. (2020). PPGPass : Nonintrusive and secure mobile two-factor authentication via wearables. Dans *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, pp. 1917–1926. IEEE.

Cifrasoft (2019). *Sound login two factor authentication*. Repéré à https://soundlogin.com/

Cipriani, J. (2022). Google signs up 150 million people for two-factor authentication : What it is, how it works. *CNET. Retrieved January*, *14*.

Deloffre, X. (2025). *Double Authentification*. Repéré à https://facemweb.com/blog/creation-site/double-authentification-2fa/

Ghose, N., Gupta, K., Lazos, L., Li, M., Xu, Z. & Li, J. (2023). ZITA : zero-interaction two-factor authentication using contact traces and in-band proximity verification. *IEEE Transactions on Mobile Computing*, *23*(5), 6318–6333.

Gupta, B., Prajapati, V., Nedjah, N., Vijayakumar, P., El-Latif, A. A. A. & Chang, X. (2023). Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (TMIS). *Neural Computing and Applications*, *35*(7), 5055–5080.

Han, D., Chen, Y., Li, T., Zhang, R., Zhang, Y. & Hedgpeth, T. (2018). Proximity-proof : Secure and usable mobile two-factor authentication. Dans *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, pp. 401–415.

He, Y., Wang, W., Teng, Y., Wang, Q., Wang, M. & Lin, J. (2022). ABLE : Zero-effort two-factor authentication exploiting BLE co-location. Dans *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 992–997. IEEE.

Hong, E., Lee, S., Oh, M.-K. & Seo, S.-H. (2021). Two-factor device DNA-based fuzzy vault for industrial IoT device security. *Ieee Access*, *9*, 99009–99023.

Husa, E. & Tourani, R. (2021). Vibe : An implicit two-factor authentication using vibration signals. Dans *2021 IEEE Conference on Communications and Network Security (CNS)*, pp. 236–244. IEEE.

Jayson, S. (2020). The 2020 State of Password and Authentication Security Behaviors Report.

Karapanos, N., Marforio, C., Soriente, C. & Capkun, S. (2015). {Sound-Proof} : Usable {Two-Factor} authentication based on ambient sound. Dans *24th USENIX security symposium (USENIX security 15)*, pp. 483–498.

Kim, S.-K., Yeun, C. Y., Damiani, E. & Lo, N.-W. (2019). A machine learning framework for biometric authentication using electrocardiogram. *Ieee Access*, *7*, 94858–94868.

Lamiche, I., Bin, G., Jing, Y., Yu, Z. & Hadid, A. (2019). A continuous smartphone authentication method based on gait patterns and keystroke dynamics. *Journal of Ambient Intelligence and Humanized Computing*, *10*(11), 4417–4430.

Lee, K., Esposito, C. & Lee, S.-Y. (2019). Vulnerability analysis challenges of the mouse data based on machine learning for image-based user authentication. *IEEE Access*, *7*, 177241–177253.

Lee, W.-H. & Lee, R. B. (2017). Implicit smartphone user authentication with sensors and contextual machine learning. Dans *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 297–308. IEEE.

Maynes, M. (2019). *One simple action you can take to prevent 99.9 percent of attacks on your accounts—microsoft. com*.

Oren, Y. & Arad, D. (2022). Toward usable and accessible two-factor authentication based on the piezo-gyro channel. *IEEE Access*, *10*, 19551–19557.

Petsas, T., Tsirantonakis, G., Athanasopoulos, E. & Ioannidis, S. (2015). Two-factor authentication : is the world ready ? Quantifying 2FA adoption. Dans *Proceedings of the eighth european workshop on system security*, pp. 1–7.

Punithavathi, P., Geetha, S., Karuppiah, M., Islam, S. H., Hassan, M. M. & Choo, K.-K. R. (2019). A lightweight machine learning-based authentication framework for smart IoT devices. *Information Sciences*, *484*, 255–268.

Ren, Y., Wen, P., Liu, H., Zheng, Z., Chen, Y., Huang, P. & Li, H. (2021). Proximity-echo : Secure two factor authentication using active sound sensing. Dans *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*, pp. 1–10. IEEE.

Shah, S. W. & Kanhere, S. S. (2017). Wi-auth : WiFi based second factor user authentication. Dans *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems : Computing, Networking and Services*, pp. 393–402.

Shrestha, B., Mohamed, M. & Saxena, N. (2019). ZEMFA : zero-effort multi-factor authentication based on multi-modal gait biometrics. Dans *2019 17th international conference on privacy, security and trust (PST)*, pp. 1–10. IEEE.

Shrestha, B., Shirvanian, M., Shrestha, P. & Saxena, N. (2016). The sounds of the phones : Dangers of zero-effort second factor login based on ambient audio. Dans *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 908–919.

Shrestha, P. & Saxena, N. (2018). Listening watch : Wearable two-factor authentication using speech signals resilient to near-far attacks. Dans *Proceedings of the 11th ACM conference on security & privacy in wireless and mobile networks*, pp. 99–110.

Stackoverflow (2025). *Architecture MVC*. Repéré à https://stackoverflow.com/questions/5966905/what-is-the-right-mvc-diagram-for-a-web-application

Tang, C., Cui, Z., Chu, M., Lu, Y., Zhou, F. & Gao, S. (2022). Piezoelectric and machine

learning based keystroke dynamics for highly secure user authentication. *IEEE Sensors Journal*, *23*(20), 24070–24077.

Wang, M., Zhu, W.-T., Yan, S. & Wang, Q. (2018). SoundAuth : Secure zero-effort two-factor authentication based on audio signals. Dans *2018 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9. IEEE.

Zhang, J. & Zhang, Q. (2021). Comment on "Secure and Lightweight Conditional Privacy-Preserving Authentication for Securing Traffic Emergency Messages in VANETs". *IEEE Transactions on Information Forensics and Security*, *18*, 1037–1038.

Zhao, T., Wang, Y., Liu, J., Cheng, J., Chen, Y. & Yu, J. (2021). Robust continuous authentication using cardiac biometrics from wrist-worn wearables. *IEEE Internet of Things Journal*, *9*(12), 9542–9556.