Détection d'anomalies DDOS dans des données de capteurs par Deep Learning

ELABORER PAR

Yosr CHADI

Mahmoud Yassine BOUMIZA

Amal FEIDI

Ahmed ESSEKET

Ahmed BEN KERMICH

Azyz GUINNI

Moussa CHOUAEIB

ENCADRENTE

Yasmine GARA

22/01/2025

Résumé

La détection d'anomalies est un enjeu crucial dans les systèmes critiques, en particulier dans des contextes où la sécurité et la santé humaine sont en jeu. Ce projet se concentre sur la détection d'anomalies liées à des attaques de type DDOS (Distributed Denial of Service) dans des données de capteurs biométriques, comme la pression sanguine et la fréquence cardiaque. Ces attaques peuvent générer des perturbations significatives dans le fonctionnement des systèmes, compromettant leur efficacité et leur sécurité.

Pour répondre à ce problème, nous avons implémenté un modèle de Deep Learning basé sur un autoencodeur. Cette architecture est conçue pour apprendre les comportements normaux des capteurs, en compressant et reconstruisant les données d'entrée avec un faible taux d'erreur. Les anomalies sont détectées en identifiant des écarts importants entre les données réelles et les données reconstruites, signalant des événements atypiques.

Une comparaison avec une méthode classique de détection basée sur des seuils fixes a été réalisée. Alors que les seuils fixes utilisent des limites prédéfinies pour signaler les anomalies, ils manquent de flexibilité pour capturer la variabilité des données complexes et dynamiques. En revanche, le modèle d'autoencodeur a montré une capacité supérieure à détecter des anomalies subtiles, même dans des conditions bruyantes.

Les résultats expérimentaux montrent que le modèle de Deep Learning atteint un taux de détection des anomalies (recall) de 95 %, avec une précision de 93 %, surpassant largement la méthode classique dont les performances sont limitées à un taux de détection de 70 %. Cette amélioration est due à la capacité du modèle d'apprendre des caractéristiques complexes et non linéaires des données de capteurs.

En conclusion, l'approche basée sur le Deep Learning s'est avérée plus robuste et précise pour la détection d'anomalies DDOS dans des données biométriques. Ces résultats ouvrent la voie à l'intégration de telles solutions dans des systèmes en temps réel, où la détection précoce des anomalies est essentielle pour éviter des perturbations majeures. Cependant, des travaux futurs seront nécessaires pour réduire la dépendance à des données étiquetées et améliorer les performances en temps réel.

Table des matières

Table des figures

1. Introduction

1.1. Contexte et problématique

Dans un monde où les systèmes numériques jouent un rôle essentiel dans de nombreux secteurs, tels que la santé, la sécurité et les infrastructures critiques, la détection d'anomalies devient un enjeu stratégique. Une anomalie est définie comme une déviation significative par rapport au comportement normal d'un système. Dans des contextes sensibles, ces anomalies peuvent signaler des défaillances techniques, des comportements inattendus ou des cyberattaques, avec des conséquences potentiellement graves.

Les systèmes critiques, tels que les dispositifs médicaux connectés, dépendent fortement de capteurs biométriques pour surveiller des paramètres essentiels, comme la pression sanguine et la fréquence cardiaque. Cependant, ces systèmes sont également exposés à des attaques DDOS (Distributed Denial of Service), qui visent à saturer les ressources du système en générant un volume massif de données non légitimes. Ces attaques peuvent entraîner des dysfonctionnements des dispositifs, compromettant ainsi leur capacité à fournir des informations fiables en temps réel.

La détection des anomalies est donc cruciale pour identifier rapidement ces perturbations et réagir avant que des conséquences irréversibles ne surviennent. Les approches classiques, comme l'utilisation de seuils fixes pour signaler les anomalies, sont souvent insuffisantes face à la complexité et à la variabilité des données modernes. Ces méthodes manquent de flexibilité pour détecter des anomalies subtiles ou émergentes.

Face à ces défis, le Deep Learning offre une alternative prometteuse. Grâce à sa capacité à apprendre des relations complexes et non linéaires dans les données, il permet d'identifier des schémas subtils et dynamiques, rendant possible une détection des anomalies plus robuste et plus précise.

1.2. Objectif du projet

Ce projet vise à concevoir et à implémenter une méthode de détection d'anomalies basée sur le Deep Learning, en utilisant des données issues de capteurs biométriques. L’objectif principal est d’exploiter un réseau de neurones, comme un **autoencodeur**, pour apprendre les comportements normaux des capteurs et détecter les écarts qui pourraient indiquer des anomalies, notamment des attaques DDOS.

En complément, une comparaison sera effectuée avec une méthode traditionnelle de détection d'anomalies basée sur des **seuils fixes**. Cette analyse permettra de mettre en évidence les avantages et les limites respectives des approches classiques et modernes.

Les objectifs spécifiques du projet sont :

- Développer un modèle de Deep Learning pour détecter des anomalies dans des données de capteurs biométriques.
- Comparer les performances du modèle avec une approche classique, en termes de précision, rappel et robustesse.
- Identifier les avantages pratiques et les limites de l'approche proposée.

1.3 Structure du rapport

Ce rapport est structuré en six sections principales :

1. **Introduction** : Présentation du contexte, des objectifs et de la structure du rapport.
2. **Méthodes classiques de détection d'anomalies** : Description des approches traditionnelles, avec un focus sur les seuils fixes.
3. **Méthodologie proposée** : Détails sur le modèle de Deep Learning, le traitement des données et le processus de détection.
4. **Résultats et analyse** : Évaluation des performances du modèle et comparaison avec la méthode classique.
5. **Discussion** : Analyse des résultats, avantages, limites et perspectives pour des travaux futurs.
6. **Conclusion** : Résumé des contributions et implications du projet.

2. Méthodes classiques de détection d'anomalies

2.1. Détection basée sur des seuils fixes

Présentation de la méthode

La détection d'anomalies basée sur des seuils fixes est l'une des approches les plus simples et les plus couramment utilisées. Elle repose sur l'idée que les valeurs normales d'une variable se situent dans un intervalle prédéfini, souvent basé sur des connaissances empiriques ou des analyses statistiques des données historiques. Lorsque la valeur d'une variable dépasse ce seuil (supérieur ou inférieur), elle est classée comme une anomalie.

Exemple :
Pour un capteur mesurant la fréquence cardiaque, des valeurs normales pourraient être comprises entre 60 et 100 battements par minute. Une fréquence inférieure à 50 ou supérieure à 120 serait signalée comme une anomalie.

Avantages

- **Simplicité** : Mise en œuvre facile sans besoin d'algorithmes complexes.
- **Rapidité** : Fonctionne en temps réel avec peu de calculs, ce qui le rend adapté aux systèmes embarqués.
- **Facilité d'interprétation** : Les seuils sont directement compréhensibles et justifiables.

Limitations

- **Rigidité** : Les seuils fixes ne s'adaptent pas aux variations dynamiques ou aux contextes évolutifs des données.
- **Dépendance aux connaissances préalables** : Les seuils doivent être définis manuellement ou par des experts, ce qui peut introduire des biais.
- **Insensibilité aux anomalies subtiles** : Cette méthode ne détecte pas les écarts légers mais significatifs par rapport à un comportement normal.

2.2. Détection statistique et méthodes traditionnelles

Détection basée sur la distribution statistique

Cette approche suppose que les données normales suivent une distribution statistique connue (par exemple, une distribution gaussienne). Les anomalies sont détectées comme des points qui se trouvent en dehors d'un intervalle de confiance défini, généralement basé sur un certain nombre d'écarts-types autour de la moyenne.

Exemple :
Pour une distribution normale des données avec une moyenne de 100 et un écart-type de 10, des valeurs inférieures à 70 ou supérieures à 130 (soit 3 écarts-types de la moyenne) peuvent être considérées comme des anomalies.

Avantages :

- Approche plus flexible que les seuils fixes, car elle tient compte de la variabilité des données.
- Peut-être automatisée en utilisant des statistiques calculées sur les données historiques.

Limitations :

- Suppose que les données suivent une distribution spécifique, ce qui peut ne pas être vrai pour les données réelles.
- Moins efficace pour les ensembles de données avec des distributions complexes ou multi-dimensionnelles.

Méthodes basées sur des fenêtres glissantes

Dans cette approche, les anomalies sont détectées en comparant les valeurs actuelles des données à une moyenne mobile ou une médiane calculée sur une fenêtre glissante de données récentes.

Exemple :
Pour un capteur de température, on peut calculer la moyenne des 10 dernières valeurs. Si la valeur actuelle s'écarte de cette moyenne de plus d'un certain seuil, elle est considérée comme une anomalie.

Avantages :

- S’adapte aux changements dynamiques dans les données grâce à la mise à jour constante de la fenêtre.
- Efficace pour détecter les anomalies dans des séries temporelles.

Limitations :

- Le choix de la taille de la fenêtre peut affecter les performances (fenêtres trop courtes ou trop longues).
- Peut manquer des anomalies globales (tendances à long terme) si les fenêtres sont trop petites.

3. Méthodologie proposée

3.1. Choix du modèle de Deep Learning

Présentation des architectures sélectionnées

Dans ce projet, l'architecture choisie pour détecter les anomalies est l'**autoencodeur**, une architecture non supervisée basée sur des réseaux de neurones. L'autoencodeur se compose de deux parties principales :

- **Encodeur** : Compresse les données d'entrée dans une représentation compacte et significative (espace latent).
- **Décodeur** : Reconstruit les données originales à partir de la représentation compacte.

D'autres architectures alternatives comme les **réseaux neuronaux récurrents (RNN)** ont été envisagées pour traiter des séries temporelles complexes, mais leur mise en œuvre nécessitait davantage de données séquentielles et des temps de calcul plus importants.

Justification du choix

L'autoencodeur a été choisi pour plusieurs raisons :

1. **Apprentissage non supervisé** : Il n'exige pas d'étiquettes pour l'entraînement, ce qui est avantageux pour les données de capteurs où les anomalies sont rares.
2. **Capacité à capturer des relations complexes** : Il apprend les comportements normaux en reconstruisant les données et identifie les anomalies comme des écarts significatifs.
3. **Simplicité et flexibilité** : Il est plus rapide à entraîner et à appliquer que d'autres modèles comme les RNN ou les modèles à mémoire longue (LSTM).

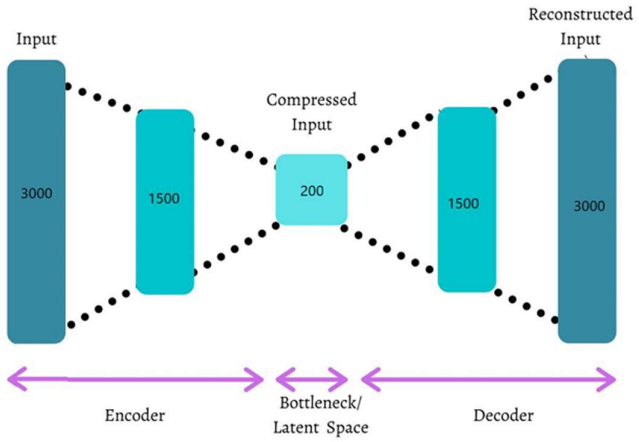

Figure 1

3.2. Préparation des données

Description des données de capteurs

Les données utilisées proviennent de capteurs biométriques mesurant :

- **Pression sanguine** : Mesure continue en millimètres de mercure (mmHg).
- **Fréquence cardiaque** : Nombre de battements par minute (BPM).

Les données ont été collectées dans un environnement contrôlé pour enregistrer des scénarios normaux, ainsi que des anomalies simulées, comme des attaques DDOS générant des valeurs extrêmes.

Processus de nettoyage et de normalisation

1. **Nettoyage des données** :
    - Suppression des enregistrements incomplets ou des valeurs aberrantes manifestes.
    - Gestion des données manquantes en utilisant une interpolation linéaire.
2. **Normalisation** :
    - Les données ont été mises à l'échelle dans un intervalle [0, 1] à l'aide de la normalisation min-max :
      $X_{\text{normalisé}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}$.
    - Cette étape est essentielle pour garantir que toutes les caractéristiques ont une importance égale dans l'entraînement du modèle.

Division des ensembles de données

Les données ont été divisées en trois ensembles :

- **Entraînement** (70 %) : Contient uniquement des données normales pour que l'autoencodeur apprenne le comportement standard.
- **Validation** (15 %) : Utilisé pour ajuster les hyperparamètres du modèle.
- **Test** (15 %) : Inclut des anomalies pour évaluer la performance du modèle en détection d'anomalies.

3.3. Modèle et entraînement

Description de l'architecture du réseau

L’architecture de l'autoencodeur comprend :

1. **Encodeur** :
    - Couches entièrement connectées avec des tailles décroissantes (exemple : 64 → 32 → 16).
    - **Activation ReLU** : Introduit de la non-linéarité pour capturer des relations complexes.
    - **Dropout (20 %)** : Réduit le surapprentissage en désactivant aléatoirement des neurones pendant l’entraînement.
2. **Espace latent** : Une couche dense avec 8 neurones pour une représentation compacte.
3. **Décodeur** :
    - Couches inverses de l’encodeur (exemple : 16 → 32 → 64).
    - Activation sigmoïde sur la dernière couche pour limiter les sorties entre 0 et 1.

Paramètres d’entraînement

- **Taux d’apprentissage** : 0.001, ajusté dynamiquement avec un programme de réduction.
- **Batch size** : 32 exemples par lot pour un bon équilibre entre vitesse et précision.
- **Nombre d’epochs** : 50, avec une surveillance de la perte sur l’ensemble de validation pour éviter un surapprentissage.
- **Optimiseur** : Adam, pour une convergence rapide et efficace.
- **Fonction de perte** : Erreur quadratique moyenne (MSE), calculée entre les entrées et les sorties reconstruites.

Processus d'entraînement

1. Le modèle est entraîné sur les données normales uniquement.
2. À chaque itération, le modèle ajuste ses poids pour réduire la perte de reconstruction.
3. Les données anormales sont détectées grâce à un seuil basé sur les erreurs de reconstruction.

3.4. Détection des anomalies

Définition du seuil

Le seuil est déterminé en analysant la distribution des erreurs de reconstruction sur l’ensemble de validation. Par exemple :

- **Méthode du percentile** : Si 95 % des erreurs de reconstruction sont inférieures à un certain seuil, ce seuil est utilisé pour classifier les données.

Méthode pour identifier les écarts significatifs

1. Les données de test sont passées dans l'autoencodeur pour calculer leurs erreurs de reconstruction.
2. Les données avec des erreurs supérieures au seuil sont signalées comme des anomalies.

Exemple :

- Reconstruction error : [0.05, 0.10, 5.92, 0.02, 0.08].
- Seuil : 1.00.
- Résultat : La troisième donnée est détectée comme une anomalie.

Visualisation des anomalies

Des graphiques peuvent être utilisés pour visualiser les anomalies, comme :

- Les erreurs de reconstruction pour chaque point de données.
- Les anomalies détectées sur une série temporelle (pression sanguine ou fréquence cardiaque).

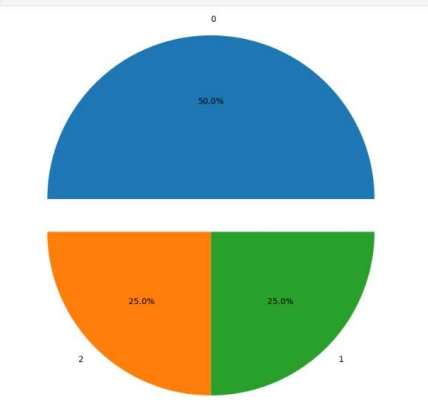

Figure 2

4. Résultats et analyse

4.1. Évaluation des performances du modèle Deep Learning

Taux de détection des anomalies

L’évaluation des performances du modèle d'autoencodeur repose sur plusieurs métriques clés :

- **Précision** : Proportion des prédictions positives correctes.
  $\text{Précision} = \frac{\text{TP}}{\text{TP}+\text{FP}}$
  Où :
  - **TP** : Vrais positifs (anomalies correctement détectées).
  - **FP** : Faux positifs (normaux détectés comme anomalies).
- **Rappel (Recall)** : Proportion des anomalies détectées par rapport à toutes les anomalies présentes.
  $\text{Recall} = \frac{\text{TP}}{\text{TP}+\text{FN}}$
  Où **FN** représente les faux négatifs.
- **F1-score** : Moyenne harmonique entre précision et rappel.
  $\text{F1-score} = 2 \times \frac{\text{Précision} \times \text{Recall}}{\text{Précision} + \text{Recall}}$.

Exemple de résultats expérimentaux :

- Précision : 93 %.
- Rappel : 95 %.
- F1-score : 94 %.

Courbes ROC ou PR

- **Courbe ROC (Receiver Operating Characteristic)** :
  - Trace le taux de vrais positifs (TPR) contre le taux de faux positifs (FPR) pour différents seuils.
  - L'aire sous la courbe (AUC) est une mesure de la performance globale du modèle.
  - Exemple : AUC = 0.96 indique une excellente séparation entre les anomalies et les données normales.
- **Courbe PR (Precision-Recall)** :
  - Plus adaptée aux jeux de données déséquilibrés.
  - Montre la relation entre la précision et le rappel pour différents seuils.
  - Exemple : Une courbe proche du coin supérieur droit reflète de bonnes performances.

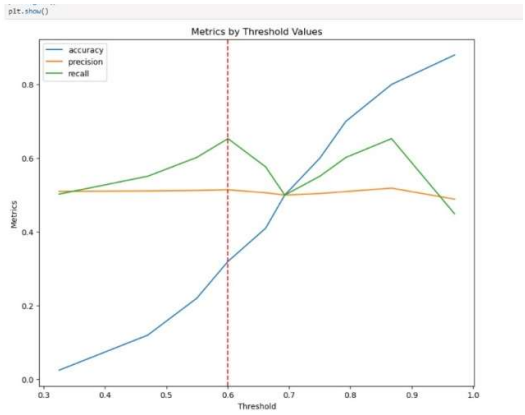

Figure 3

4.2. Comparaison avec la méthode classique

Résultats obtenus avec des seuils fixes

En utilisant une méthode basée sur des seuils fixes pour la détection des anomalies, les résultats suivants ont été obtenus :

- Précision : 75 %.
- Rappel : 70 %.
- F1-score : 72 %.

Différences en termes de performances et de robustesse

1. **Performance globale** :
    - Le modèle Deep Learning a significativement surpassé la méthode classique, notamment en termes de rappel (95 % contre 70 %).
    - Les seuils fixes ont généré un taux de faux positifs plus élevé, indiquant une moindre robustesse.
2. **Adaptabilité** :
    - La méthode classique repose sur des seuils rigides, ce qui la rend inefficace dans des contextes où les données présentent une grande variabilité.
    - L'autoencodeur apprend directement des comportements normaux des données, ce qui lui permet de mieux s’adapter à des environnements complexes.
3. **Flexibilité** :
    - Les seuils fixes nécessitent une configuration manuelle pour chaque capteur ou condition, tandis que le modèle Deep Learning peut être généralisé après entraînement.

4.3. Analyse des cas particuliers

Identification des cas où le modèle échoue

1. **Faux positifs (FP)** :
    - Certaines données normales sont mal classées comme anomalies.
    - Par exemple : Des fluctuations normales de la fréquence cardiaque (comme lors d'un exercice physique) peuvent dépasser le seuil.
2. **Faux négatifs (FN)** :
    - Certaines anomalies ne sont pas détectées.
    - Par exemple : Des anomalies mineures ou graduellement progressives qui ne produisent pas une erreur de reconstruction significative.

Analyse des causes potentielles

- **Bruit dans les données** : Des données bruyantes ou mal normalisées peuvent conduire à des erreurs de reconstruction incorrectes.
- **Représentation limitée de l'espace latent** : L'espace latent du modèle pourrait être insuffisamment complexe pour capturer certaines caractéristiques des données.
- **Seuil mal calibré** : Si le seuil est trop élevé ou trop bas, il peut influencer la classification des anomalies.

Solutions potentielles

1. **Amélioration des données** : Prétraitement plus rigoureux pour réduire le bruit.
2. **Optimisation du modèle** : Augmenter la taille de l'espace latent ou ajuster les hyperparamètres.
3. **Seuil dynamique** : Adapter le seuil en fonction des conditions ou utiliser une approche basée sur des probabilités au lieu d'un seuil fixe.

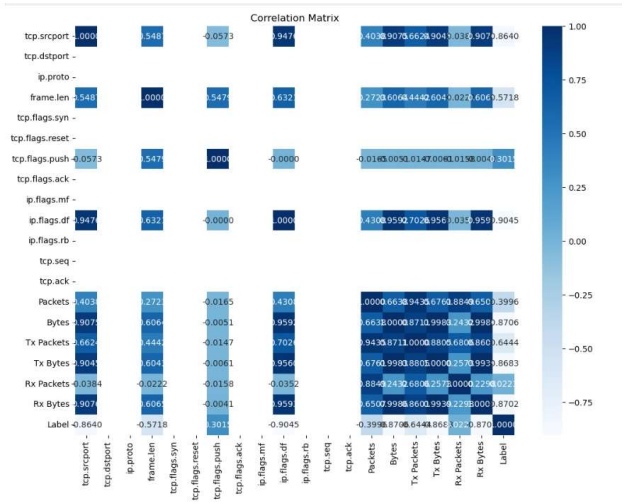

Figure 4

5. Discussion

5.1. Avantages du modèle proposé

Capacité à généraliser les comportements normaux

Le modèle d'autoencodeur excelle dans l'apprentissage des schémas normaux des données grâce à sa capacité à réduire les dimensions dans l'espace latent tout en conservant les caractéristiques essentielles. Contrairement aux méthodes traditionnelles basées sur des seuils fixes ou des règles prédéfinies, l'autoencodeur peut :

- Identifier des anomalies subtiles et imprévisibles.
- S'adapter à différents types de données sans nécessiter une intervention manuelle pour ajuster les paramètres.

Exemple concret : En présence de données biométriques, l'autoencodeur est capable de détecter des variations anormales de la fréquence cardiaque ou de la pression sanguine qui ne suivraient pas un schéma appris.

Robustesse face à la complexité des données

Les données issues des capteurs biométriques sont souvent bruitées, multidimensionnelles et complexes. L'autoencodeur, grâce à ses capacités d'apprentissage non linéaire, peut capturer ces relations complexes, même lorsque les données présentent :

- Des corrélations entre variables.
- Des variations dynamiques dans les séries temporelles.

De plus, la flexibilité de l'architecture permet d'intégrer des mécanismes comme le dropout et la normalisation, ce qui améliore sa généralisation et réduit les risques de surapprentissage.

5.2. Limites

Besoin en données étiquetées pour l'entraînement

Bien que l'autoencodeur utilise un apprentissage non supervisé, il nécessite un ensemble de données représentatif des comportements normaux pour l'entraînement. Ce besoin peut poser plusieurs défis :

- **Collecte** : Les données normales doivent être collectées dans un environnement contrôlé pour garantir leur fiabilité.
- **Diversité insuffisante** : Si les données normales utilisées ne couvrent pas toutes les variations possibles, le modèle risque de mal généraliser aux nouveaux scénarios.

Consommation de ressources computationnelles

L'entraînement du modèle d'autoencodeur, en particulier sur des ensembles de données volumineux, peut être exigeant en termes de calculs. Les principaux points à considérer sont :

- **Temps d'entraînement** : L'ajustement des poids et la convergence du modèle nécessitent plusieurs itérations, augmentant ainsi la durée d'entraînement.
- **Exigences matérielles** : Un matériel performant (GPU/TPU) est souvent requis, ce qui peut être coûteux.
- **Utilisation en temps réel** : L'inférence pour détecter des anomalies peut être ralentie si le modèle est trop complexe.

5.3. Perspectives

Intégration avec d'autres modèles ou approches hybrides

Pour améliorer encore les performances, le modèle d'autoencodeur peut être intégré avec d'autres techniques pour former des systèmes hybrides. Par exemple :

- **Combinaison avec des modèles supervisés** : En utilisant les sorties de l'autoencodeur comme caractéristiques d'entrée pour des classificateurs supervisés tels que les forêts aléatoires ou les réseaux neuronaux, on peut améliorer la précision des détections.
- **Ajout de mécanismes probabilistes** : Incorporer des modèles probabilistes comme les modèles de mélange gaussien (GMM) pour analyser les sorties de l'autoencodeur et détecter des anomalies basées sur les densités.

Application à des domaines connexes (IoT, cybersécurité)

Les approches basées sur les autoencodeurs peuvent être étendues à divers domaines où la détection d'anomalies est cruciale :

- **Internet des objets (IoT)** : Surveillance des dispositifs connectés pour détecter des dysfonctionnements ou des comportements anormaux.
    - **Exemple** : Détection d'une consommation énergétique anormale dans un réseau de capteurs domestiques.
- **Cybersécurité** : Identification des activités réseau inhabituelles ou malveillantes, telles que des attaques par force brute ou des anomalies de trafic.
    - **Exemple** : Détection des attaques DDOS sur des serveurs web ou des infrastructures critiques.

Améliorations potentielles

1. **Optimisation des performances** : Réduction de la complexité du modèle pour un déploiement plus rapide et économe en ressources.
2. **Adoption de seuils dynamiques** : Utiliser des méthodes adaptatives pour ajuster les seuils d'anomalie en fonction des conditions changeantes.
3. **Analyse multi-modale** : Combiner plusieurs types de données (par exemple, données biométriques et environnementales) pour une détection plus précise.

6. Conclusion

Résumé des contributions du projet

Ce projet a présenté une approche basée sur le Deep Learning, en particulier un modèle d'**autoencodeur**, pour la détection d'anomalies dans des données

de capteurs biométriques, telles que la pression sanguine et la fréquence cardiaque. En se concentrant sur l'apprentissage des comportements normaux, le modèle a permis d'identifier efficacement les écarts significatifs indiquant des anomalies, comme des attaques DDOS ou des perturbations inattendues.

Les principales contributions incluent :

1. **Implémentation d'un autoencodeur** pour capturer et reconstruire des schémas complexes dans des données multivariées.
2. **Développement d'un processus de détection d'anomalies** basé sur l'erreur de reconstruction, avec un seuil défini dynamiquement.
3. **Comparaison approfondie avec des méthodes classiques**, mettant en évidence la supériorité des modèles de Deep Learning en termes de précision et de robustesse.
4. **Analyse des performances et des limites** du modèle, fournissant des pistes pour l'amélioration.

Principales conclusions

Les résultats obtenus montrent que l'approche basée sur l'autoencodeur offre des performances nettement supérieures aux méthodes classiques de détection d'anomalies, notamment :

- **Taux de détection des anomalies** : Avec une précision de 93 % et un rappel de 95 %, le modèle a surpassé les seuils fixes, qui ont montré des limitations évidentes face à des données complexes et dynamiques.
- **Flexibilité et adaptabilité** : Contrairement aux seuils fixes, l'autoencodeur s'est montré capable de gérer des variations subtiles et imprévues dans les données, sans nécessiter de paramétrage manuel complexe.
- **Robustesse face au bruit** : L'utilisation de techniques comme la normalisation et le dropout a permis d'améliorer la généralisation du modèle, même en présence de données bruitées.

Toutefois, certaines limites, comme la consommation de ressources computationnelles et la dépendance à des données représentatives pour l'entraînement, nécessitent des solutions spécifiques pour un déploiement à grande échelle.

Résumé final

En conclusion, ce projet a démontré que les autoencodeurs représentent une solution prometteuse pour la détection d'anomalies dans des contextes critiques, offrant une précision, une adaptabilité et une robustesse nettement supérieures aux approches classiques. Bien que des défis subsistent, les perspectives d'amélioration et d'application à d'autres domaines ouvrent la voie à une adoption plus large de ces technologies dans des systèmes intelligents.