الجمهورية الشعبية الديمقراطية الجزائرية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي ٠08 ماي 1945٠ بسيدي بلعباس
École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès

Mémoire de Fin d'étude

En Vue de l'obtention du diplôme d'**ingénieur d'état**
Filière : **Informatique**
Spécialité : **Système d'Information et Web (SIW)**

Thème

A Machine Learning Based Intrusion Detection System for Internet of Medical Things

---

Présenté par :

- M. LAHMAR Mohammed Abdrrahim
- Mlle. DJELLOUL DAOUADJI Fadela

Soutenu le : **03/07/2023**

Devant le jury composé de :

Mme. ANANI Djihed	Président
M. KHALDI Miloud	Encadreur
Mlle. BABA-AHMED Manel	Examinateur

Année Universitaire : 2022/2023

Acknowledgments

We first want to express our sincere thanks to Allah for helping us and giving us the patience and motivation to complete this work.

We would particularly like to thank our supervisor, **Dr. Miloud KHALDI**, for the help he has given us, for his patience and encouragement. His critical eyes were very valuable in structuring the work and improving the quality of the different sections.

We would also like to thank our promoter **Pr. Sidi Mohammed BENSLIMANE** for his immense help, the quality of his follow-up as well as for all the advices and informations he gave us with a degree of patience and professionalism.

Big thanks to our **parents** who have taught, worked on and improved, loved, cared, sacrificed and shared everything with us, may God bless them.

We would like to express our sincere thanks to the members of the jury for the honour they have done us by taking the time to read and evaluate this work. We would also like to thank the pedagogical and administrative team of the ESI-SBA 8-mai-1945 for their efforts to offer us an excellent training.

Big thanks to all my **teachers** who have taught, worked on and improved our skills to reach such a respectful level, may God bless you all and your families with health and success.

Abstract

The Internet of Things is an extension of the current Internet to all objects that can communicate, directly or indirectly, with electronic equipment that is connected to the Internet. IoT offers services in many areas related to human life such as health, transport, home, smart cities, etc. The security of these components and data transfers is a major issue.

In this final project, we propose a Machine Learning based intrusion detection system for Healthcare Applications, where a user submits requests to complete a task. Intruders can submit false requests to disrupt the operation of this system. Their detection requires the development of a reliable security system capable of detecting any intrusion during all phases of the execution process.

Keywords : Machine Learning (ML), Intrusion Detection System (IDS), Internet of Medical Things (IoMT), Healthcare, Anomaly Detection, Features Selection.

Résumé

L'Internet des Objets est une extension de l'Internet actuel où tous les objets pouvant communiquer, de manière directe ou indirecte, avec des équipements électroniques eux-mêmes connectés à l'Internet. IoT offre des services dans beaucoup de domaines liés à la vie humaine comme la santé, le transport, à domicile, les cités intelligentes, etc. La sécurité de ces composants et des transferts de ces données est un enjeu majeur.

Dans ce projet de fin d'études, nous proposons un système de détection d'intrusion basé sur l'apprentissage automatique pour les applications de santé, où un utilisateur soumet des demandes pour accomplir une tâche. Des intrus peuvent soumettre des fausses requêtes pour perturber le fonctionnement de ce système. Leurs détections nécessitent le développement d'un système de sécurité fiable et capable de détecter toute intrusion durant toutes les phases de processus d'exécution.

Mots clés : Apprentissage automatique, Système de Détection d'Intrusions, Internet des Objets Médicaux, Soins de santé, Détection d'anomalie, Sélection des attributs.

مُلخص

إن إنترنت الأشياء هو امتداد للإنترنت الحالي لجميع الأشياء التي يمكنها الاتصال ، بشكل مباشر أو غير مباشر، مع الأجهزة الإلكترونية المتصلة بالإنترنت. تقدم إنترنت الأشياء خدمات في العديد من المجالات المتعلقة بحياة الإنسان مثل الصحة ، والنقل ، والمنزل ، والمدن الذكية ، وما إلى ذلك. تعد حماية هذه المكونات وعمليات نقل البيانات قضية رئيسية.
في هذا المشروع النهائي ، نقترح نظامًا لاكتشاف التسلل قائمًا على التعلم الآلي في بيئة إنترنت الأشياء الطبية، حيث يقوم المستخدم بإرسال طلبات لإنجاز مهمة. يمكن للمتطفلين تقديم طلبات كاذبة لتعطيل عمل هذا النظام. يتطلب اكتشافهم تطوير نظام أمان موثوق به قادر على اكتشاف أي اختراق خلال جميع مراحل عملية التنفيذ.

الكلمات المفتاحية : التعلم الآلي ، نظام كشف الإختراق ، أنترنت الأشياء الطبية ، الرعاية الصحية ، اكتشاف الأخطاء ، اختيار الميزات .

List of Abbreviations and Acronyms

1. **ML :** Machine Learning.
2. **IDS :** Intrusion Detection System.
3. **IoT :** Internet of Things.
4. **IoMT :** The Internet of Medical Things.
5. **AIDS :** Anomaly Intrusion Detection Systems.
6. **IPS :** Intrusion Prevention System.
7. **LSTM :** Long Short-Term Memory.
8. **NIDS :** Network Intrusion Detection System.
9. **HIDS :** Host Intrusion Detection System.
10. **SIDS :** Signature-based Intrusion Detection System.
11. **AI :** Artificial Intelligence.
12. **DL :** Deep Learning.
13. **KNN :** K Nearest Neighbors.
14. **DT :** Decision Tree.
15. **RF :** Random Forest.
16. **XGBoost :** Extreme gradient boosting.
17. **LR :** Logistic Regression.
18. **SVM :** Support Vector Machines.

19. **DQN :** Deep Q Network.
20. **SARSA :** State-Action-Reward-State-Action.
21. **TN :** True Negatives.
22. **TP :** True Positives.
23. **FN :** False Negatives.
24. **FP :** False Positives.
25. **Acc :** Accuracy.
26. **ROC :** Receiver Operator Characteristic.
27. **MAE :** Mean Absolute Error.
28. **CNNs :** Convolutional Neural Networks.
29. **RNNs :** Recurrent Neural Networks.
30. **GANs :** Generative Adversarial Networks .
31. **MLPs :** Multi-layer Perceptrons.
32. **AB :** AdaBoost.
33. **GBM :** Gradient Boosted Machine.
34. **AUC :** Ope Discriminant Analysis.
35. **ETC :** Extremely Randomized Trees.
36. **CART :** Classification And Regression Trees.
37. **CFS :** Correlation-based Feature Selection.
38. **IG :** Information Gain.
39. **GR :** Gain Ratio.
40. **PCA :** Principal Component Analysis.
41. **GA :** Genetic Algorithm.
42. **PSO :** Particle Swarm Optimization.

43. **ABC :** Artificial Bee Colony.
44. **SAE :** Stacked Autoencoder.
45. **SU :** Symmetrical Uncertainty.
46. **MCC :** Matthews Correlation Coefficient.
47. **DR :** Detection Rate.
48. **FAR :** False Alarm Rate.
49. **APIs :** Application Programming Interfaces.
50. **ACCS :** Australian Centre for Cyber-Security.
51. **DoS :** Denial of Service.
52. **U2R :** User to Root.
53. **R2L :** Remote to Local.
54. **CV :** Cross Validation.
55. **NSL-KDD :** Network Security Lab - Knowledge Discovery and Data mining.
56. **UNSW-NB15 :** University of New South Wales-Network Based 15.
57. **GUI :** Graphic User Interface.
58. **EHRs :** Electronic Health Records.