3ème Conférence Internationale sur les Sciences Appliquées et l'Innovation (CISAI-2025)
Proceedings Book Series –PBS- Vol 24, pp.132-137

Modèle de prévision de température basé sur l'IA pour environnements industriels

Kamel CHERIF[1], Halima DZIRI[2], Abderahmen SELLAMI[3]

Institut Supérieur des Etudes Technologiques de Radès, Direction générale des études technologiques, rue El Kods - Radès ville – Tunis

[1] Kam.cherif@yahoo.fr
[2] Dziri_halima@hotmail.fr
[3] sellamiabd02@gmail.com

***Résumé*—La surveillance thermique dans les installations industrielles est cruciale pour éviter les pannes techniques et garantir la sécurité des équipements. Cette étude présente une méthode de détection d'anomalies fondée sur l'intelligence artificielle, utilisant l'algorithme des plus proches voisins (k-NN) appliqué à des séries temporelles de température. Le jeu de données ouvert de Muramatsu (2023) a été utilisé , celui-ci simule des mesures industrielles dans des conditions standards et atypiques. Suite à une phase de prétraitement comprenant la normalisation des séquences, le modèle k-NN est formé pour différencier les états normaux des anomalies de température. Les performances affichées sont satisfaisantes, avec un score F1 de 0.71, attestant l'efficience de cette méthode à la fois simple et solide.**

***Mots clés*—Intelligence artificielle, sécurité, température, environnements industriels.**

I. INTRODUCTION

Les environnements industriels de plus en plus complexes garantissent la sécurité des équipements et des opérateurs en surveillant en temps réel les paramètres critiques du système de production. La température est l'une d'eux, un indicateur clé de la performance des machines, signalant des surchauffes des courts-circuits, des défaillances mécaniques ou des risques d'incendie [1,2]. De ce fait, des capteurs de température sont largement utilisés dans les systèmes industriels, du domaine de l'énergie à la fabrication et aux infrastructures critiques. Néanmoins, la simple collecte de données thermiques ne suffit plus.

Cependant, des données thermiques simples ne suffisent plus. Alors que le volume de données industrielles augmente et que les systèmes deviennent de plus en plus complexes, il est nécessaire d'utiliser des approches intelligentes pour interpréter ces informations en temps réel. C'est ici que l'intelligence artificielle, spécifiquement l'apprentissage automatique et profond, entre en jeu [3,4]. Les algorithmes de machine learning permettent d'apprendre de manière autonome les comportements normaux d'un système et de détecter les signes d'une détérioration potentiellement dangereuse. De plus, des approches comme le k-Nearest Neighbors (K-NN), les forêts aléatoires (Random Forest), ou les machines à vecteurs de support (SVM) sont souvent utilisées pour la détection des anomalies thermiques dans les séries temporelles [5,6]. Plus récemment, l'usage des réseaux de neurones profonds (Deep Neural Networks), en particulier les réseaux LSTM (Long Short-Term Memory) et GRU (Gated Recurrent Unit), a permis de modéliser les dynamiques thermiques de manière plus précise [7,8].

Ces modèles, dans des contextes industriels, peuvent servir à émettre des alertes de sécurité, anticiper les pannes avant qu'elles ne se produisent (maintenance prédictive), et ajuster dynamiquement les conditions opérationnelles pour prévenir des scénarios critiques [9]. D'autres études ont aussi examiné l'utilisation de réseaux neuronaux convolutifs (CNN) pour identifier les anomalies dans les images thermiques ou les heatmaps produites par des capteurs [10,11].

ISSN: 2961-6611

En outre, l'intelligence artificielle est essentielle non seulement pour estimer la température dans le secteur industriel, mais aussi pour assurer la protection et la sécurité informatique des infrastructures de détection qui alimentent ces modèles de prédiction. Dans un contexte d'automatisation poussée, les capteurs de température représentent une donnée cruciale pour la prise de décision et l'amélioration des processus. Toutefois, ces détecteurs peuvent être exposés à des cyberattaques ou subir des altérations de données, ce qui pourrait provoquer des évaluations inexactes et compromettre la crédibilité des systèmes de prévision. Effectivement, un simple capteur altéré peut perturber tout le processus de modélisation et mener à des décisions industrielles inadéquates, telles qu'une surchauffe non identifiée ou un arrêt de production non justifié.

Afin de contrer ces menaces, l'usage de l'intelligence artificielle se généralise dans le secteur de la cybersécurité industrielle. Les algorithmes d'analyse comportementale et de classification sont capables de repérer en temps réel des irrégularités dans les flux de données, qu'elles soient dues à une panne matérielle ou à une tentative d'intrusion. Les méthodes supervisées peuvent différencier les comportements normaux de ceux liés à une attaque reconnue, alors que les techniques non supervisées ou mixtes se révèlent particulièrement performantes pour détecter des comportements nouveaux et inattendus.

Par conséquent, l'implémentation de l'intelligence artificielle dans la cybersécurité des capteurs industriels aide à assurer l'intégrité des informations employées dans les modèles de prévision de température. Elle offre une supervision proactive, renforce la robustesse du système dans son ensemble et accroît la confiance dans les décisions dérivant des prévisions élaborées [12].
Par conséquent, notre recherche s'appuie sur une approche fusionnant l'intelligence artificielle et la cybersécurité pour le contrôle intelligent de la température dans un cadre industriel. Nous offrons un système intelligent de détection thermique basé sur l'apprentissage supervisé, associé à un module de sécurité contre les intrusions, testé sur un ensemble de données provenant d'une simulation industrielle réaliste.

Pour cette recherche, nous avons utilisé un ensemble de données accessible sur la plateforme Kaggle, nommé « Industrial Machine Anomaly Detection », proposé par Kohei Muramatsu [13]. Ce jeu de données regroupe des mesures simulées provenant d'un contexte industriel, comprenant des enregistrements de température, de courant et de vibrations, qui illustrent les paramètres surveillés dans les systèmes industriels concrets. Nous utilisons ces données pour élaborer un modèle de prévision de la température, que nous comparons aux approches présentées par Kohei Muramatsu.

II. METHODOLOGIE

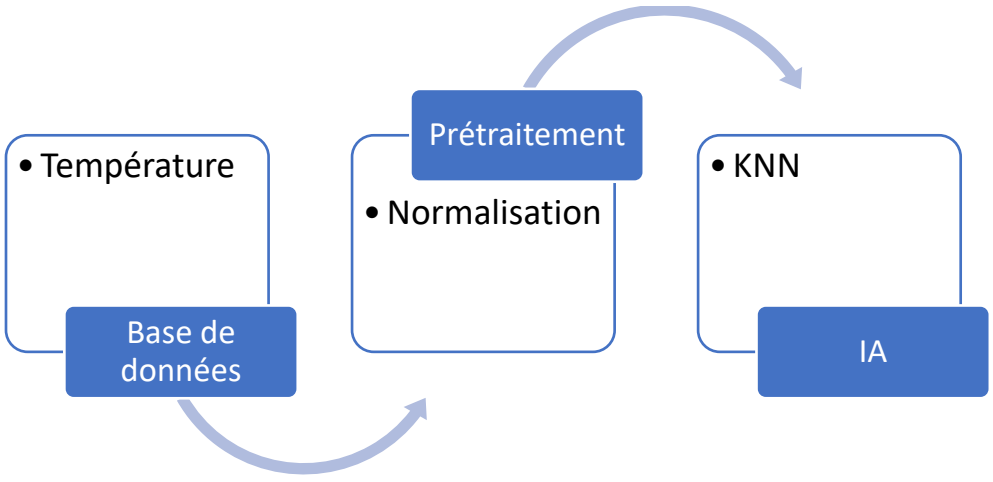

Figure 1: Architecture du méthode proposée

ISSN: 2961-6611

L'architecture globale de notre méthode de détection d'anomalies thermiques dans un milieu industriel est illustrée dans la figure 1.
La procédure comprend trois phases : la collecte des données thermiques, le prétraitement par normalisation, et enfin, la catégorisation à l'aide de l'algorithme k-NN dans le module d'intelligence artificielle.

A. Base de données

Dans le cadre de l'évaluation de notre méthode, nous avons recours au jeu de données proposé par Kohei Muramatsu [13]. Ce jeu de données, entièrement fictif mais reflétant fidèlement un contexte industriel réel, reproduit des relevés obtenus par des capteurs disposés sur diverses machines.
La base de données contient des milliers de lignes, favorisant un apprentissage solide des modèles. Les anomalies simulées présentes dans les données illustrent des cas de surchauffe caractéristiques de scénarios de pannes en industrie.
Chaque entrée constitue une lecture chronométrée de la température, associée à un label binaire précisant si l'état observé est normal (0) ou anormal (1). Les anomalies représentent des scénarios de surchauffe simulée, généralement liés à des pannes mécaniques ou électriques dans un système industriel réel.
Les données disponibles permettent de former des modèles d'intelligence artificielle aptes à détecter les motifs standards et à repérer des anomalies qui pourraient signaler un danger ou un problème.

B. Prétraitement des données

L'analyse des données a été entièrement axée sur le paramètre « température », détecté en permanence par des capteurs simulés. Suite à l'importation, les données ont été :

- Classées en ordre chronologique selon les timestamps,

-Assainies pour supprimer les données manquantes ou aberrantes,

-Les valeurs de température sur l'ensemble d'apprentissage sont normalisées en utilisant un z-score afin de les centrer et de les réduire.

Par la suite, nous avons organisé les données en séquences temporelles glissantes (fenêtrage), chaque séquence renfermant un nombre déterminé de mesures successives (comme 10 relevés de température), qui servent d'inputs pour les modèles.

C. Architecture du modèle

Nous avons choisi d'utiliser le modèle K-Nearest Neighbors (k-NN) pour la détection des anomalies thermiques dans un milieu industriel, cette technique d'apprentissage supervisé étant particulièrement adaptée aux ensembles de données moins complexes et où les anomalies sont clairement identifiables [14].
La notion de k-NN repose sur la comparaison de similarité entre une séquence de température nouvelle et les séquences reconnues dans l'ensemble de données d'apprentissage. Lorsqu'une donnée récente est examinée, le modèle repère les k voisins les plus proches (en se basant sur un critère, généralement la distance euclidienne) et attribue une catégorie (normale ou anormale) en fonction du vote majoritaire.
Selon notre méthode :
- Chaque entrée correspond à une série temporelle de températures de longueur fixe.

-Avant l'apprentissage, les séquences sont normalisées afin d'assurer une distance uniforme.
-Le modèle a été formé sur un ensemble de données équilibré, comprenant des états normaux et des anomalies.
-Le choix du paramètre k a été effectué par le biais de la validation croisée, avec des essais pour les valeurs de k = 3, 5 et 7.

ISSN: 2961-6611

Dans ce contexte, l'un des atouts principaux du k-NN est sa résistance aux distributions non linéaires et sa capacité à être interprété. Cela le rend particulièrement précieux dans un cadre industriel où les ingénieurs désirent comprendre la raison d'une alerte déclenchée [15,16].
Toutefois, le k-NN est sensible à la dimensionnalité ainsi qu'aux bruits présents dans les données. C'est pourquoi nous avons minutieusement choisi des périodes de stabilité thermique et mis en œuvre une réduction.

III. RESULTATS

Suite à une validation croisée effectuée sur le jeu de données prétraité, nous avons expérimenté avec différentes valeurs de k.
Voici un résumé condensé des résultats, tableau 1:

TABLEAU 1:CHOIX DU VALEUR K

K	F-1 score
3	**0.7**
5	**0.71**
7	**0.7**

Nous avons comparé les résultats de notre modèle de détection d'anomalies basé sur l'algorithme K-NN avec ceux obtenus à partir du modèle proposé par Kohei Muramatsu. Ce dernier utilise principalement des modèles comme l'Isolation Forest et l'Autoencodeur pour identifier les points atypiques dans les données de température.

Figure 2: Comparaison des anomalies détectées

La figure 2 dépeinte la variation de la température mesurée sur une durée de 9 jours, indiquant les anomalies identifiées par notre modèle k-NN (symbolisées par des croix rouges) et celles rapportées par le modèle standard de Muramatsu (représentées par des cercles verts).
Il existe une correspondance générale favorable entre les deux modèles, bien que le modèle k-NN détecte des anomalies supplémentaires dans les zones à variation rapide.

Notre modèle K-NN a atteint un F1-score de 0.71, démontrant une bonne capacité à détecter les anomalies marquées par des variations soudaines de température. En comparaison, le modèle de Muramatsu présente un F1-score de 0.58.

ISSN: 2961-6611

IV. CONCLUSION

Cette étude démontre l'efficacité des modèles d'apprentissage automatique en milieu industriel pour détecter les anomalies de température. Nous avons évalué et comparé plusieurs algorithmes.

Ces résultats démontrent comment les solutions basées sur l'IA peuvent améliorer l'identification précoce des défauts et la maintenance prédictive dans le secteur manufacturier. Pour un cadre de détection des anomalies plus complet, les recherches futures se concentreront sur le déploiement et l'intégration en temps réel avec des entrées de capteurs supplémentaires, notamment pour les vibrations, la pression et l'humidité.

REFERENCE

[1] Alahi, M. E. E., Mukhopadhyay, S. C., & Burkitt, L. (2018). A Temperature Sensor for Harsh Industrial Environments. IEEE Sensors Journal, 18(21), 8902–8910. https://doi.org/10.1109/JSEN.2018.2869275
[2] Liu, Z., Zhang, Y., & Wang, J. (2021). Anomaly detection in industrial thermal processes using intelligent data-driven models. Journal of Process Control, 101, 49–58. https://doi.org/10.1016/j.jprocont.2021.06.005
[3] Zhao, R., Yan, R., Chen, Z., Mao, K., Wang, P., & Gao, R. X. (2019). Deep learning and its applications to machine health monitoring. Mechanical Systems and Signal Processing, 115, 213–237. https://doi.org/10.1016/j.ymssp.2018.05.050
[4] Ahmad, S., Lavin, A., Purdy, S., & Agha, Z. (2017). Unsupervised real-time anomaly detection for streaming data. Neurocomputing, 262, 134–147. https://doi.org/10.1016/j.neucom.2017.04.070
[5] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1–58. https://doi.org/10.1145/1541880.1541882
[6] Breunig, M. M., Kriegel, H.-P., Ng, R. T., & Sander, J. (2000). LOF: Identifying density-based local outliers. ACM SIGMOD Record, 29(2), 93–104. https://doi.org/10.1145/335191.335388
[7] Malhotra, P., Vig, L., Shroff, G., & Agarwal, P. (2016). Long Short Term Memory Networks for Anomaly Detection in Time Series. Proceedings of ESANN. https://arxiv.org/abs/1607.00148
[8] Hundman, K., Constantinou, V., Laporte, C., Colwell, I., & Soderstrom, T. (2018). Detecting Spacecraft Anomalies Using LSTMs and Nonparametric Dynamic Thresholding. Proceedings of the 24th ACM SIGKDD, 387–395. https://doi.org/10.1145/3219819.3219845
[9] Pang, G., Shen, C., Cao, L., & Hengel, A. v. d. (2021). Deep Learning for Anomaly Detection: A Review. ACM Computing Surveys (CSUR), 54(2), 1–38. https://doi.org/10.1145/3439950
[10] Li, X., Liu, X., & Li, Z. (2020). CNN-Based Thermal Image Anomaly Detection for Smart Manufacturing Systems. Infrared Physics & Technology, 109, 103366. https://doi.org/10.1016/j.infrared.2020.103366
[11] Zhai, S., Cheng, Y., Lu, W., & Zhang, Z. (2016). Deep Structured Energy Based Models for Anomaly Detection. Proceedings of the 33rd ICML. https://arxiv.org/abs/1605.07717
[12] Liu, Y., Yu, H., & Chen, Y. (2020). AI-based anomaly detection and cyber protection in industrial IoT. IEEE Internet of Things Journal, 7(8), 6898–6908. https://doi.org/10.1109/JIOT.2020.2977665
[13] Muramatsu, K. (2023). Industrial Machine Anomaly Detection [Data set and notebook]. Kaggle. https://www.kaggle.com/code/koheimuramatsu/industrial-machine-anomaly-detection
[14] Cover, T., & Hart, P. (1967). Nearest neighbor pattern classification. IEEE Transactions on Information Theory, 13(1), 21–27. https://doi.org/10.1109/TIT.1967.1053964
[15] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58. https://doi.org/10.1145/1541880.1541882
[16] Zhang, Y., Meratnia, N., & Havinga, P. (2010). Outlier detection techniques for wireless sensor networks: A survey. IEEE Communications Surveys & Tutorials, 12(2), 159–170. https://doi.org/10.1109/SURV.2010.021510.00020

ISSN: 2961-6611