Analyse bibliométrique de la cybersécurité dans l'IoT industriel

Ignacio J. Dasso
Nantes Université
CNRS, IETR, UMR 6164
F-85000 La Roche-sur-Yon, France

Sébastien Maudet
Nantes Université
CNRS, IETR, UMR 6164
F-85000 La Roche-sur-Yon, France

Renzo E. Navas
IMT Atlantique
IRISA, UMR CNRS 6074
F-35700 Rennes, France

Guillaume Andrieux
Nantes Université
CNRS, IETR, UMR 6164
F-85000 La Roche-sur-Yon, France

***Abstract*—L'IoT industriel (IIoT) fait référence à l'interconnection de machines dans l'environnement de production des entreprises. En adoptant les caractéristiques de l'IoT, l'IIoT a également hérité de ses risques en matière de cybersécurité. De nombreux efforts ont été déployés par la communauté scientifique pour faire face à ces multiples aspects. Dans cet article, nous présentons une étude bibliomètrique de la cybersécurité dans l'IIoT et les résultats nous permettent d'établir un panorama de l'état de la recherche sur les dix dernières années. Cette vue actualisée permet également d'améliorer la compréhension du domaine, d'apprécier les efforts réalisés et d'observer les tendances en terme de recherche.**

***Index Terms*—internet des objets, IoT, IIoT, industrie, cybersécurité, bibliométrie**

I. Introduction

L'Internet des objets (IoT) est une aggrégation de capteurs, de systèmes embarqués, de capacités informatiques, de technologies de communication et d'Internet [1]. Un nombre incalculable d'applications ont trouvé des solutions par le développement de l'IoT. L'IoT industriel (IIoT) correspond à l'adoption de l'IoT par l'industrie.

L'inclusion d'applications IIoT dans des processus critiques a entraîné la nécessité d'assurer la sécurité pour garantir la robustesse et prévenir l'indisponibilité du système. Par conséquent, la cybersécurité dans l'IIoT apparaît comme un domaine d'étude exigeant un traitement spécifique. L'objectif de ce travail est de présenter de manière structurée, un panorama de la cybersécurité dans l'IIoT.

II. Travaux connexes

Différents inventaires ou études bibliométriques traitent de la cybersécurité dans la littérature scientifique. Les auteurs de l'article [2] abordent la détection d'anomalies dans l'industrie à l'aide de dispositifs IoT et d'algorithmes d'apprentissage automatique. L'article [3] étudie l'efficacité de l'utilsation de la blockchain dans un milieu industriel. Dans l'article [4], les auteurs analysent la gestion des risques cyber dans l'industrie, à travers l'utilisation des technologies de sécurité pour l'IoT. Les auteurs de la référence [5] passent en revue les différentes publications du domaine et les regroupent selon leurs thématiques et leurs pays de provenance. La référence [6] identifie différents aspects du domaine et recommande l'utilisation de l'apprentissage automatique et de la blockchain dans la résolution des problèmes liés à la cybersécurité dans l'IIoT.

Ces différents inventaires ou études bibliométriques abordent la cyber-sécurité d'un point de vue de l'IoT en général ou d'un thème spécifique de l'industrie. Il n'existe pas, à notre connaissance, d'étude qui couvre l'état de la recherche dans la cybersécurité de l'IIoT en tant que sujet principal. Pour combler cette lacune, nous avons réalisé une étude bibliométrique de la littérature scientifique afin de présenter une vue d'ensemble de la cybersécurité dans l'IIoT.

III. Methodologie

Cette étude bibliométrique est basée sur une analyse quantitative des publications de la dernière décennie.

A. Questions de recherche

Les questions suivantes représentent les objectifs fixés :

RQ1. Quels sont les principaux axes de recherche dans le domaine de la cybersécurité de l'IIoT ?
RQ2. Quels sont les sujets les plus fréquents en fonction de l'occurrence des mots-clés ?
RQ3. Quels sont les éditeurs qui ont le plus contribué ?
RQ4. Quelles sont les publications les plus citées ?
RQ5. Quelles sont les tendances en matière de publications associées aux sujets les plus fréquents ?

Afin de réaliser l'étude, les articles doivent être sélectionnés dans une base de données selon un processus qui s'appuie sur des requêtes de recherche et un cadre temporel. Les articles sont ensuite évalués en fonction de mots-clés, de l'année de publication et du nombre de citations. Ces paramètres constituent la base à partir de laquelle il est possible de créer des graphiques et des tableaux qui permettront par la suite d'analyser les tendances.

B. Sélection des articles dans la littérature

Les mots-clés qui ont été choisis pour décrire la "cybersécurité de l'IIoT" sont les suivants : "industry", "IIoT", "Internet of Things", "IoT", "cybersecurity" et "security". La base de données est Scopus en raison de la quantité massive de sources ($N_s = 47680$) qu'elle contient, ainsi que la présence des éditeurs les plus pertinents du domaine (ACM, IEEE, Elsevier, Wiley, MPDI) [7]. Les recherches sont effectuées sur la dernière décennie, de 2014 à 2024.

Les requêtes doivent être compatibles avec l'interface offerte par Scopus. Une requête est développée de manière à

ce qu'elle corresponde au plus grand nombre possible de résultats. Par conséquent, les mots-clés tels que "industry" ou "industrial" doivent être inclus, de même que "IIoT", mais ils ne sont pas obligatoires. Le même critère s'applique à "IoT" et à "Internet of Things". La requête 1 (Q1) représente l'aboutissement de cette réflexion.

Listing 1. Requête principale (Q1).

```
TITLE-ABS-KEY ( industr* OR iiot ) AND (
TITLE-ABS-KEY ( "internet of things" OR iot )) AND (
TITLE-ABS-KEY ( cybersecurity OR security )) AND (
PUBYEAR > 2013 ) AND ( PUBYEAR < 2025 ) AND (
LIMIT-TO ( LANGUAGE , "English" ))
```

Les informations extraites de Scopus sont ensuite traitées afin de les adapter à l'outil graphique. Les critères de traitement doivent répondre aux attentes de la phase de préparation de l'information. L'identification des groupes s'appuie sur les mots-clés. Par conséquent, tout article exporté ne comportant pas au moins un des mots-clés est écarté.

C. Détermination des groupes

Les groupes sont identifiés sur une carte de visualisation élaborée par la solution VOSviewer, en se basant sur la cooccurrence des mots-clés. La cooccurrence est représentée sous la forme de lignes reliant les différents concepts. Plus la ligne est épaisse, plus le nombre de cooccurrences est élevée. Sur la carte, chaque mot-clé est représenté par un noeud. La taille des noeuds est proportionnelle au nombre d'utilisation d'un concept comme mot-clé. Le paramètre de résolution du logiciel VOSviewer permet de gérer le nombre de grappes, qui évolue proportionnellement à la valeur de ce paramètre.

D. Identification des éditeurs

De nombreux éditeurs ont contribué à la publication d'article sur la cybersécurité dans l'IIoT. Les exportations de Scopus permettent d'identifier les principaux éditeurs ainsi que les taux de publication annuels.

E. Identification des publications les plus citées

Les publications les plus citées ont un contenu qui est reconnu par des lecteurs spécialistes du domaine. Les publications obtenues dans Scopus sont triées en fonction du nombre moyen de citations par an. Ce tri tient compte du fait que les publications plus anciennes bénéficient de plus de temps pour être citées, ce qui normalise les résultats. L'année 2025 est l'année de référence. Le facteur de normalisation est obtenu en soustrayant l'année de publication. Ainsi, les publications de 2024 ont un nombre de citations divisé par 1 ($2025 - 2024 = 1$), tandis que les publications de 2014 ont un nombre de citations divisé par 11 ($2025 - 2014 = 11$).

F. Identification des surveys les plus cités

Un survey est un article d'analyse des différents sujets qui composent une thématique de recherche. Ils offrent généralement un état de l'art et précisent les défis à relever. Les survey les plus citées sont classés en fonction du nombre moyen de citations par an, en limitant le corpus aux survey et études similaires. La requête 2 (Q2) est le résultat de cette réflexion.

Listing 2. Requête de recherche des survey (Q2)

```
TITLE-ABS-KEY ( industr* OR iiot ) AND (
TITLE-ABS-KEY ( "internet of things" OR iot )) AND (
TITLE-ABS-KEY ( cybersecurity OR security )) AND (
PUBYEAR > 2021 ) AND (PUBYEAR < 2025 ) AND (
TITLE (review OR survey OR map* ) ) AND (
TITLE (iiot or cybersecurity )) AND (
LIMIT-TO ( LANGUAGE,"English" ) )
```

IV. Resultats

La première requête (Q1) a fourni 12 573 résultats. Elle a été exécutée le 22 janvier 2025.

A. RQ1. Quels sont les principaux axes de recherche dans le domaine de la cybersécurité de l'IIoT ?

La cooccurrence des mots clés est repésentée sur la carte de visualisation de la figure 1. Les groupes identifiés sont les suivants :

1. "Computing and security" (15 items) : "blockchain", "security", "cryptography", "authentification", "decision processes", "data administration" et "computing technologies".
2. "Network awareness" (14 items) : "network security", "industrial IoT", "intrusion detection" et "learning technologies".
3. "Industrial embedded systems" (13 items) : "industrial embedded system" et "cyber-physical systems", "artificial intelligence", "security of systems and data", et "big data".
4. "Automation and networks" (8 items) : "automation", "network architecture", "intelligent buildings", wireless sensor network" et "energy usage".

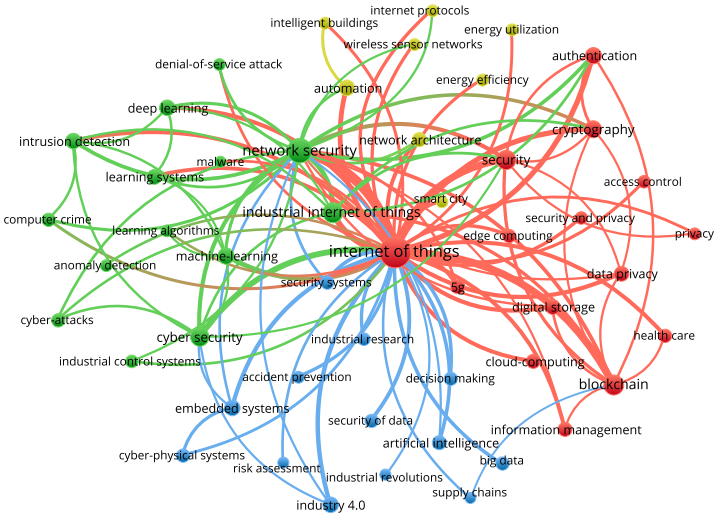

Fig. 1. Carte de visualisation des mots-clés en réseau.

Les mots-clés “cybersecurity” et “Industrial Internet of Things” sont les plus pertinents. Pour le mot-clé “cybersecurity”, les principales connexions qui apparaissent sont “network security”, “machine learning”, “intrusion detection”, “embedded systems”, “Industry 4.0” et “cyber-attacks”. “Industrial IoT” est relié “network security”, “blockchain”, “cryptography”, “authentication”, “intrusion detection” et “deep learning”. A partir de ces résultats, les observations suivantes s’imposent :

- les deux mots-clés appartiennent au groupe 2 “Network awarness” ;
- les deux mots-clés sont liés à la sécurité des réseaux et à la détection d’intrusion ;
- le mot-clé “cybersécurité” est plus relié aux mots-clés du groupe 3 “Industrial embedded systems” que le mot-clé “IoT industriel” ;
- le mot-clé “Internet des objets industriel” est plus relié aux mots-clés du groupe 1 “Computing and security” que le mot-clé “cybersecurity” ;
- les deux mots-clés sont reliés avec une technologie liée à l’apprentissage : “cybersecurity” avec “machine learning” et “Industrial IoT” avec “deep learning”.

B. RQ2. Quels sont les sujets les plus fréquents en fonction de l’occurrence des mots-clés ?

Les 20 sujets les plus fréquents sont synthétisés dans le tableau I. Le mot-clé “IoT” (6697 occurrences) arrive en tête du classement, suivi par l’item “network security” (3293 occurrences). Les sujets “Industrial IoT” (1630 occurrences), “blockchain” (1614 occurrences), “security” (1498 occurrences) et “cybersecurity” (1307 occurrences) viennent ensuite avec plus de 1000 occurrences.

TABLE I
LES 20 SUJETS LES PLUS FRÉQUENTS

Occ.	Sujet	Occ.	Sujet
6997	1 internet of things	737	3 embedded systems
3293	2 network security	724	2 deep learning
1630	2 industrial iot	699	4 automation
1614	1 blockchain	694	3 industry 4.0
1498	1 security	642	1 data privacy
1307	2 cybersecurity	638	1 digital storage
938	1 cryptography	625	2 learning systems
868	1 authentication	549	1 cloud-computing
858	2 machine-learning	543	4 network architecture
768	2 intrusion detection	527	1 information management

Sur les 20 sujets, 9 sont dans le groupe 1 “Computing and security” et 7 dans le groupe 2 “Network awareness”.

C. RQ3. Quels sont les éditeurs qui ont le plus contribué ?

Les éditeurs qui ont le plus contribué sont IEEE (39,0%) et Springer (16,8%), avec plus de 55% du total des publications. Le tableau II liste les éditeurs responsables d’au moins 2% du total des publications.

La figure 2 représente le nombre de publications par année en distinguant les principaux contributeurs. La dernière année est tracée en pointillés car le nombre final de publications n’est pas disponible. IEEE est l’éditeur dominant, suivi en deuxième position par Springer. Les publications augmentent d’année en année, mais avec un ratio plus faible pour 2024.

TABLE II
PRINCIPAUX ÉDITEURS DANS LE DOMAINE DE LA CYBERSÉCURITÉ POUR L’IIOT DE 2014 À 2024[a]

Éditeur	Nombre de publications	Pourcentage
IEEE	4901	39.0%
Springer	2118	16.8%
Elsevier	964	7.7%
MDPI	760	6.0%
ACM	379	3.0%
Wiley	284	2.3%
Autres	3167	25.2%

[a]Le 23 janvier 2025.

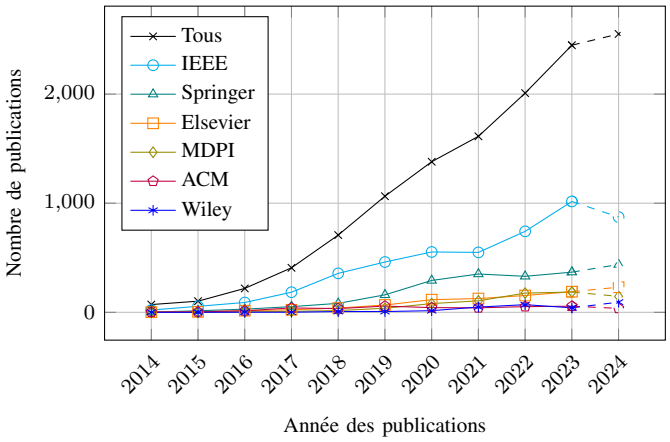

Fig. 2. Nombre de publications par éditeur et par an (le 23 janvier 2025).

D. RQ4. Quelles sont les articles les plus cités ?

Le tableau III contient la liste des 10 articles les plus cités en moyenne, entre 2014 et 2024 (survey compris). Le tableau IV contient la liste des 10 survey les plus citées en moyenne, pour la période allant de 2022 à 2024.

Le nombre de citations varie entre 719 et 2461 pour l’ensemble des articles et entre 14 et 190 pour les survey uniquement. L’examen des tableaux III et IV fait apparaitre le mot-clé “blockchain” comme le sujet le plus fréquent, avec 6 occurrences.

E. RQ5. Quelles sont les tendances en matière de publications associées aux sujets les plus fréquents ?

La réponse à la question 2 fournit une liste des sujets les plus populaires sur la base de l’occurrence des mots clés. La question 5 s’appuie sur des mots-clés capables de modifier le concept de “cybersécurité dans l’IIoT”, à savoir “blockchain”, “cryptography”, “authentication”, “machine learning”, “intrusion detection”, et “embedded systems”. Chaque mot-clé est utilisé pour identifier le nombre de publications par an.

TABLE III
LES 10 PUBLICATIONS LES PLUS CITÉES DE 2014 À 2024[a]

Nombre de citations par an	Nombre de citations	Titre de la publication
615	2461	Machine Learning: Algorithms, Real-World Applications and Research Directions [8]
255	1788	Industrial internet of things: Challenges, opportunities, and directions [9]
253	1266	A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems [10]
230	2302	The internet of things for health care: A comprehensive survey [11]
211	1480	On blockchain and its integration with IoT. Challenges and opportunities [12]
183	1468	DDoS in the IoT: Mirai and other botnets [13]
179	719	Federated Learning for Internet of Things: A Comprehensive Survey [14]
175	876	Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT [15]
160	961	Blockchain for Internet of Things: A Survey [16]
150	1055	The industrial internet of things (IIoT): An analysis framework [17]

[a]Le 23 janvier 2025.

TABLE IV
LES 10 SURVEY LES PLUS CITÉS DE 2022 À 2024[a]

Nombre de citations par an	Nombre de citations	Titre de la publication
63	190	Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review [18]
44	134	Cybersecurity Awareness in the Context of the Industrial Internet of Things: A Systematic Literature Review [19]
16	32	CMAF-IIoT: Chaotic Map-Based Authentication Framework for Industrial Internet of Things [20]
14	44	Secure Blockchain Middleware for Decentralized IIoT towards Industry 5.0: A Review of Architecture, Enablers, Challenges, and Directions [21]
12	36	Enhancing Cybersecurity Policies with Blockchain Technology: A Survey [22]
10	21	Cybersecurity for Blockchain-Based IoT Systems: A Review [23]
8	24	Secure Smart Healthcare Monitoring in Industrial Internet of Things (IIoT) Ecosystem with Cosine Function Hybrid Chaotic Map Encryption [24]
7	14	A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things [25]
7	23	Perspectives of Cybersecurity for Ameliorative Industry 4.0 Era: A Review-Based Framework [26]
7	14	Cybersecurity Risk Analysis in the IoT: A Systematic Review [27]

[a]Le 23 janvier 2025.

Les résultats représentés sur la figure 3 montrent que la "blockchain" est le sujet le plus fréquent, tandis que "machine learning" et "intrusion detection" sont les seuls sujets en augmentation constante par rapport au nombre de publications par an.

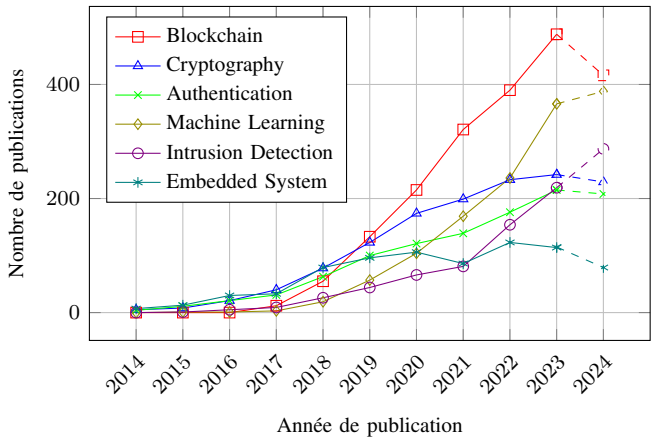

Fig. 3. Nombre de publications par sujet et par an (le 24 janvier 2024)

V. CONCLUSION ET DISCUSSIONS

Dans cet article, une étude bibliométrique est proposée afin d'offrir un panorama complet de l'état de la recherche dans la cybersécurité de l'IIoT. Cette étude est basée sur cinq questions. L'analyse des réponses de la première question a permis de répartir les sujets dans quatre groupes aux thématiques différentes : 1 "Computing and security", 2 "Network awareness", 3 "Industrial embedded system", et 4 "Automation and network". Les sujets en lien avec la sécurité des réseaux, la détection des intrusions et les technologies d'apprentissage sont plus mis en avant. La réponse à la deuxième question a renforcé la pertinence des thèmes 1 "Computing and security" et 2 "Network awareness". Les statistiques présentées à la question 3 montrent que les éditeurs IEEE et Springer ont le plus grand nombre de publications. Enfin, les réponses aux questions 4 et 5 montrent que la "blockchain", le "machine learning" et la détection d'intrusion sont les sujets les plus présents dans la littérature, avec une croissance soutenue du nombre de publications par an. La combinaison ou l'analyse individuelle de ces sujets représente une voie fructueuse pour le futur de la recherche dans les domaines de la cybersécurité de l'IIoT. Dans nos prochains travaux, nous prévoyons d'étudier la détection d'intrusion dans les réseaux IoT, puis d'améliorer cette thématique en appliquant des solutions de "Machine Learning" ou de "Blockchain".

REMERCIEMENTS

Ce travail est supporté par la région Pays-de-la-Loire et l'agglomération de La Roche-sur-Yon.

References

[1] S. N. Swamy and S. R. Kota, "An Empirical Study on System Level Aspects of Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 188 082–188 134, 2020. doi:10.1109/ACCESS.2020.3029847

[2] S. F. Chevtchenko *et al.*, "Anomaly Detection in Industrial Machinery Using IoT Devices and Machine Learning: A Systematic Mapping," *IEEE Access*, vol. 11, pp. 128 288–128 305, 2023. doi:10.1109/ACCESS.2023.3333242

[3] P. Seiler, E. Brandt, and F. Brandt, "Systematic Mapping Study on the Security and Efficiency of Blockchain in Industrial Context," *Procedia Computer Science*, vol. 217, pp. 1497–1505, 2023. doi:10.1016/j.procs.2022.12.349

[4] R. J. Raimundo and A. T. Rosário, "Cybersecurity in the Internet of Things in Industrial Management," *Applied Sciences*, vol. 12, no. 3, p. 1598, Feb. 2022. doi:10.3390/app12031598

[5] G. Mwansa and N. Mabanza, "Review of Internet of Things Security Protocols – A Bibliometric Analysis," in *2023 25th International Conference on Advanced Communication Technology (ICACT)*. Pyeongchang, Korea, Republic of: IEEE, Feb. 2023, pp. 394–400. doi:10.23919/ICACT56868.2023.10079641

[6] J. Y. Lee and J. Lee, "Current Research Trends in IoT Security: A Systematic Mapping Study," *Mobile Information Systems*, vol. 2021, pp. 1–25, Mar. 2021. doi:10.1155/2021/8847099

[7] E. B.V., "Sources," https://www.scopus.com/sources, 2024, (Accessed 2024-11-27).

[8] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Computer Science*, vol. 2, no. 3, p. 160, May 2021. doi:10.1007/s42979-021-00592-x

[9] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018. doi:10.1109/TII.2018.2852491

[10] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, Jan. 2020. doi:10.1109/JIOT.2019.2948888

[11] S. M. Riazul Islam, Daehan Kwak, M. Humaun Kabir, M. Hossain, and Kyung-Sup Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015. doi:10.1109/ACCESS.2015.2437951

[12] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and Its Integration with IoT. Challenges and Opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018. doi:10.1016/j.future.2018.05.046

[13] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017. doi:10.1109/MC.2017.201

[14] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor, "Federated Learning for Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021. doi:10.1109/COMST.2021.3075439

[15] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020. doi:10.1109/TII.2019.2942190

[16] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A Survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019. doi:10.1109/JIOT.2019.2920987

[17] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The Industrial Internet of Things (IIoT): An Analysis Framework," *Computers in Industry*, vol. 101, pp. 1–12, Oct. 2018. doi:10.1016/j.compind.2018.04.015

[18] M. Abdullahi *et al.*, "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," *Electronics*, vol. 11, no. 2, p. 198, Jan. 2022. doi:10.3390/electronics11020198

[19] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity Awareness in the Context of the Industrial Internet of Things: A Systematic Literature Review," *Computers in Industry*, vol. 137, p. 103614, May 2022. doi:10.1016/j.compind.2022.103614

[20] M. Tanveer, A. Badshah, A. U. Khan, H. Alasmary, and S. A. Chaudhry, "CMAF-IIoT: Chaotic Map-Based Authentication Framework for Industrial Internet of Things," *Internet of Things*, vol. 23, p. 100902, Oct. 2023. doi:10.1016/j.iot.2023.100902

[21] J. Leng *et al.*, "Secure Blockchain Middleware for Decentralized IIoT towards Industry 5.0: A Review of Architecture, Enablers, Challenges, and Directions," *Machines*, vol. 10, no. 10, p. 858, Sep. 2022. doi:10.3390/machines10100858

[22] A. Kumar and I. Sharma, "Enhancing Cybersecurity Policies with Blockchain Technology: A Survey," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*. Uttar Pradesh, India: IEEE, Dec. 2022, pp. 1050–1054. doi:10.1109/IC3I56241.2022.10072588

[23] R. Alajlan, N. Alhumam, and M. Frikha, "Cybersecurity for Blockchain-Based IoT Systems: A Review," *Applied Sciences*, vol. 13, no. 13, p. 7432, Jun. 2023. doi:10.3390/app13137432

[24] J. Khan *et al.*, "Secure Smart Healthcare Monitoring in Industrial Internet of Things (IIoT) Ecosystem with Cosine Function Hybrid Chaotic Map Encryption," *Scientific Programming*, vol. 2022, pp. 1–22, Mar. 2022. doi:10.1155/2022/8853448

[25] A. Alnajim, S. Habib, M. Islam, S. Thwin, and F. Alotaibi, "A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things," *Technologies*, vol. 11, no. 6, p. 161, Nov. 2023. doi:10.3390/technologies11060161

[26] A. Haleem, M. Javaid, R. P. Singh, S. Rab, and R. Suman, "Perspectives of Cybersecurity for Ameliorative Industry 4.0 Era: A Review-Based Framework," *Industrial Robot: the international journal of robotics research and application*, vol. 49, no. 3, pp. 582–597, Apr. 2022. doi:10.1108/IR-10-2021-0243

[27] T. AlSalem, M. Almaiah, and A. Lutfi, "Cybersecurity Risk Analysis in the IoT: A Systematic Review," *Electronics*, vol. 12, no. 18, p. 3958, Sep. 2023. doi:10.3390/electronics12183958