Impact of the Industrial Internet of Things (IIoT) on Cybersecurity within Industry 4.0: A Systematic Review of Literature

Sánchez Rosas, Luis Junior[1], Vega Solis, Edwin Rolando[2], Paico Egusquiza, Ayle Jarumy[2], and Mendoza Vasquez, Ari Anielka[3]

[1]*Universidad Privada del Norte, Peru, junior.sanchez@upn.edu.pe*

[2]*Universidad Tecnológica del Perú, Peru, U22212351@utp.edu.pe, U22210934@utp.edu.pe, U22211785@utp.edu.pe*

Abstract*– The accelerated growth of the Industrial Internet of Things (IIoT) has driven the need for advanced and secure anomaly detection solutions, especially in industrial environments where cybersecurity is critical. This study provides a Systematic Literature Review (SLR) guided by the PRISMA 2020 method, with the objective of identifying the impact of IIoT on cybersecurity within Industry 4.0. Thirty-two studies published between 2020 and 2024 in academic databases such as Scopus and Web of Science were reviewed. The results reveal that emerging technologies such as Blockchain, Machine Learning and Deep Learning are playing a central role in data protection and intrusion detection in IIoT systems. Blockchain has proven to be effective in ensuring data integrity and improving operational efficiency. This review highlights the importance of adopting robust cybersecurity solutions to mitigate risks and strengthen resilience in Industry 4.0 and suggests key areas for future research in this field.

***Keywords*-- IIoT, IoT, Cybersecurity, Blockchain, Industry 4.0.**

I. INTRODUCTION

Technological advancement has driven the expansion of the Internet of Things (IoT) into the industrial sector, giving rise to the Industrial Internet of Things (IIoT) [1]. This technology enables the integration of intelligent devices that process, collect, transmit and receive data in real time [2], which is essential for instant communication and collaboration between logical systems [3]. As a result, operational processes are optimized, administrative management is facilitated, and continuous and uninterrupted production is promoted.

The IIoT provides companies with unprecedented access to previously inaccessible information, thus facilitating the industry 4.0 goal of achieving smart production [4]. However, one of the main challenges in this context is the lack of cyber resilience, which introduces uncertainty about the continuity of operational processes. Therefore, it is crucial that interconnected devices are protected against unauthorized access to address vulnerabilities, reduce potential risks, and improve information access measures [5].

The IIoT connects network components through advanced communication technologies, enabling industries to efficiently monitor, share, collect and analyze data. This not only optimizes key decision making but also increases productivity and significantly improves performance [6]. In this context, it is critical to ensure data transparency, as well as to ensure protection, confidentiality and trust for both service providers and users [7], [8], [9].

The implementation of IIoT in industry poses new challenges in terms of cybersecurity [10]. These challenges include identity theft, unavailability of services, data tampering, and unauthorized disclosure of information. In response to these risks, specific regulations such as IEC 62443, which encompasses relevant standards such as ISO 27000 and IEC 61508, designed to ensure security in industrial information systems, have been proposed [11]. These standards, together with risk analysis methods and protection techniques, aim to mitigate deficiencies and strengthen system security [12].

The industrial domain requires high security standards due to the critical importance of its processes in relation to protection and industrial secrecy. Therefore, IIoT protocols must be unsurpassed in the security mechanisms they implement [13]. This not only ensures the protection of data and systems, but also fosters innovation and promotes IIoT implementation, making it easier for companies to operate more securely and optimize their processes without compromising integrity [14].

To analyze in depth the impact of IIoT on cybersecurity within Industry 4.0, a systematic literature review (SLR) was conducted, following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. This methodology ensures an exhaustive and accurate evaluation of the most relevant studies published between 2020 and 2024. As a result of this analysis, the following research questions were formulated:

What are the most used cybersecurity tools and technologies to mitigate IIoT vulnerabilities in Industry 4.0, How has the Web of Science (WoS) database facilitated the identification and analysis of key studies for systematic review on the impact of IIoT on cybersecurity in Industry 4. 0, How has the use of IIoT impacted the cybersecurity of industrial companies within Industry 4.0, How is its effectiveness evidenced, in which countries is there more interest and research activity on the impact of IIoT on cybersecurity within Industry 4.0, and in which countries is there more interest and research activity on the impact of IIoT on cybersecurity within Industry 4.0?

II. Methodology

This study has focused on a quantitative analysis to perform a comprehensive evaluation of bibliographies using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) standard, which is the preferred method for reporting items in systematic reviews and meta-analyses [15]. In 2009, the PRISMA tool was developed and published with the purpose of providing authors of systematic reviews with a structured guide that allows them to present the information collected during their research in a transparent, coherent, and detailed manner. This tool has been instrumental in improving the clarity and quality of reports in the field of systematic reviews [16].

The update of the PRISMA tool in 2020 introduced new reporting guidelines, replacing the previous version and reflecting advances in the methods used to identify, select, appraise, evaluate, and synthesize studies [17]. These changes not only adjusted the structure and presentation of the items, facilitating their implementation, but also improved the clarity and applicability of the tool in the systematic review process. It is also important to note that its implementation has promoted a higher level of transparency in the methods and results of research, strengthening confidence in the analyses presented [18].

The improvements and expansions made to the PRISMA tool have established a much more favorable environment for the development of meta-research, making it possible to optimize both the effectiveness and scope of systematic reviews [19]. These updates have made it easier for researchers to perform more rigorous and detailed analyses, which, in turn, contributes to significant progress in research quality. In addition, PRISMA ensures that systematic reviews remain comprehensive, clear and reproducible, increasing the reliability and credibility of the results obtained in the scientific field [20].

In summary, these developments evidence an increase in clarity and transparency in the elaboration of systematic reviews [21]. Finally, [22] highlights the increasingly relevant role of reviews as a research model and form of scientific publication, pointing out that the application of the PRISMA tool has contributed to the standardization and improvement of the quality of scientific studies.

A. Search Procedure

To collect articles on the impact of IIoT on cybersecurity in the context of Industry 4.0, an SLR was conducted in the Scopus and WoS databases. The objective of this search is to consolidate key information, identify previous research on the topic and locate relevant studies that provide significant insights. The search strategy was meticulously designed, using specific keywords related to artificial intelligence and academic performance, applied to the titles, abstracts and keywords of the papers, as shown in Fig. 1.

After running the search string in the aforementioned information management system, a total of 361 documents related to IIoT and cybersecurity in the context of Industry 4.0 were obtained. In addition, Table I, presented below, was used, which details the criteria used to select the documents included in the SLR.

Article title, Abstract, Keywords for Searching: ("IIoT" OR "Industrial internet of things“) AND ("Industry 4.0" AND ("Security" OR "Cyber Security"))

Fig. 1 Search string.

TABLE I
INCLUSION AND EXCLUSION RULES AND THEIR RESPECTIVE EXPLANATION

C1	Must have been published between 2020 and 2024.
C2	Must be available in “Open Access”.
C3	The document included must be an original article
C4	Articles must be written in English

B. PRISMA Approach

In step 1, articles based solely on abstract review were excluded, reducing the total to 347 studies. In step 2, duplicate articles were eliminated, given that we worked with two databases, resulting in 325 studies. Finally, in step 3, articles that did not meet the criteria established by the author were discarded, as detailed in Table I, leaving a total of 32 studies, as shown in Fig. 2.

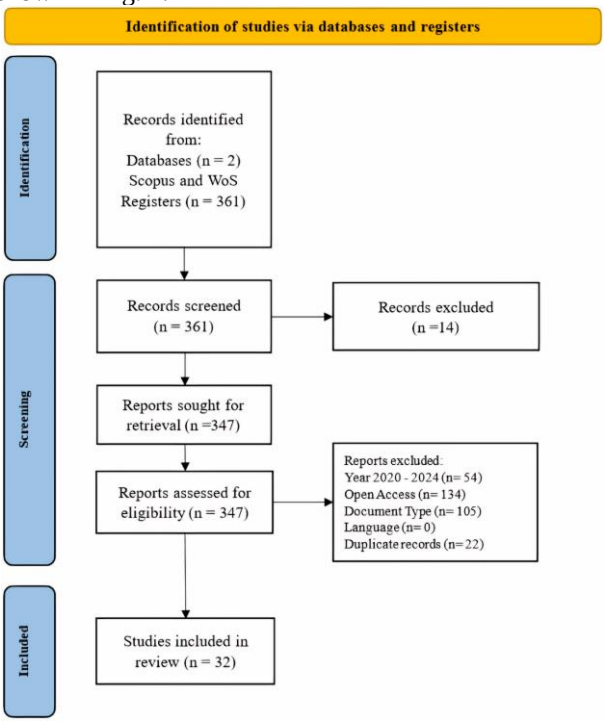

Fig. 2 Procedures for document evaluation, “Process scheme according to PRISMA”.

On the other hand, Table II presents the Scopus and WoS databases together with the final search string used. This is intended to make it easier for other researchers to replicate, use and expedite the search for information related to the research topic.

TABLE II
FINAL SEARCH STRINGS

Data base	Final Search
Scopus	(TITLE ("IIoT" OR "Industrial internet of things") AND TITLE-ABS-KEY (("Industry 4.0" AND ("Security" OR "Cyber Security")))) AND PUBYEAR > 2019 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (OA , "all"))
WoS	(ALL=("IIoT" OR "Industrial internet of things") AND ALL=("Industry 4.0" or "4.0 Industry") AND ALL=("Security" OR "Cyber Security")) AND (PY==("2024" OR "2023" OR "2022" OR "2021" OR "2020") AND DT==("ARTICLE") AND LA==("ENGLISH") AND OA==("OPEN ACCESS"))

III. Results

This section presents the findings derived from analyzing the collected studies, focusing on the use of cybersecurity tools in IIoT environments. The information is organized according to their effectiveness against different types of attacks and the metrics used for evaluation.

A. Data Overview

TABLE III
STUDIES INCLUDED IN THE SYSTEMATIC REVIEW ON IIOT AND ITS IMPACT ON CYBERSECURITY IN INDUSTRY 4.0

Authors	Name of the Studie
Wu et al. (2021) [23]	Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0
Humayun et al. (2020) [24]	Privacy protection and energy optimization for 5G-aided industrial internet of things
Hilal et al. (2022) [25]	Intelligent Deep Learning Model for Privacy Preserving IIoT on 6G Environment
Ahmed et al. (2023) [26]	Industrial Internet of Things enabled technologies, challenges, and future directions
Zhang et al. (2021) [27]	Federated Transfer Learning for IIoT Devices with Low Computing Power Based on Blockchain and Edge Computing
Bhaskaran et al. (2022) [28]	Blockchain Enabled Optimal Lightweight Cryptography Based Image Encryption Technique for IIoT
Chen et al. (2022) [29]	Enterprise Data Sharing with Privacy-Preserved Based on Hyperledger Fabric Blockchain in IIOT's Application
Wang et al. (2024) [30]	Data secure storagemechanism for IIoT based on blockchain
Qiu et al. (2023) [31]	Rendering Secure and Trustworthy Edge Intelligence in 5G-Enabled IIoT Using Proof of Learning Consensus Protocol
Lakshmanna et al. (2022) [32]	Deep Learning-Based Privacy-Preserving Data Transmission Scheme for Clustered IIoT Environment
Mahmood et al. (2024) [33]	Blockchain and PUF-based secure key establishment protocol for cross-domain digital twins in industrial Internet of Things architecture
Usman et al. (2023) [34]	Automatic Hybrid Access Control in SCADA-Enabled IIoT Networks Using Machine Learning
Idouglid et al. (2024) [35]	Next-gen security in IIoT: integrating intrusion detection systems with machine learning for industry 4.0 resilience
Aouedi et al. (2023) [36]	Federated Semisupervised Learning for Attack Detection in Industrial Internet of Things
Sasiain et al. (2020) [37]	Towards flexible integration of 5G and IIoT technologies in industry 4.0: A practical use case
Gopi et al. (2023) [38]	Intelligent Intrusion Detection System for Industrial Internet of Things Environment
Ruiz-Villafranca et al. (2023) [39]	A MEC-IIoT intelligent threat detector based on machine learning boosted tree algorithms
Rosenberger et al. (2022) [40]	Deep Reinforcement Learning Multi-Agent System for Resource Allocation in Industrial Internet of Things
Gilles et al. (2023) [41]	Securing IIoT communications using OPC UA PubSub and Trusted Platform Modules
Choudhary et al. (2020) [42]	Make-it—a lightweight mutual authentication and key exchange protocol for industrial internet of things
Mosteiro-Sanchez et al. (2020) [43]	Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0
Li et al. (2024) [44]	ASAP-IIOT: An Anonymous Secure Authentication Protocol for Industrial Internet of Things
Umran et al. (2021) [45]	Secure data of industrial internet of things in a cement factory based on a blockchain technology
Hussain et al. (2021) [46]	Secure IIoT-enabled industry 4.0
Irshad et al. (2023) [47]	SUSIC: A Secure User Access Control Mechanism for SDN-Enabled IIoT and Cyber-Physical Systems
Bicaku et al. (2020) [48]	Security standard compliance and continuous verification for Industrial Internet of Things
Alalayah et al. (2023) [49]	Optimal Deep Learning Based Intruder Identification in Industrial Internet of Things Environment
Ankita et al. (2022) [50]	Lightweight Hybrid Deep Learning Architecture and Model for Security in IIOT
Fernández-Caramés y Fraga-Lamas (2020) [51]	Use case based blended teaching of IIoT cybersecurity in the industry 4.0 era
Maghrabi et al. (2023) [52]	Golden Jackal Optimization with a Deep Learning-Based Cybersecurity Solution in Industrial Internet of Things Systems
Mantravadi et al. (2020) [53]	Securing IT/oT links for low power IIoT devices: Design considerations for industry 4.0
Vijayakumaran et al. (2020) [54]	A reliable next generation cyber security architecture for industrial internet of things environment

Firstly, Fig. 1 shows the years of scientific production of the authors selected for this review. The year with the most production was 2023 with 24 articles, representing 29% of the total, while in 2024 this number was reduced to about 21 articles, contributing 25%.

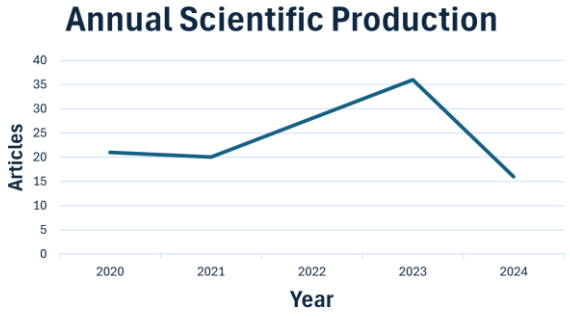

Fig. 3 Graph of the annual scientific production in relation to the years.

Next, the data presented in Fig. 2 reveal a notable concentration of research production in certain regions, especially in China, which stands out as the darkest area, indicating its high production in this field of research. In addition, Spain is the European country with the highest number of studies, although it is also important to highlight the contribution of South American countries, particularly Brazil, which has 19 contributions.

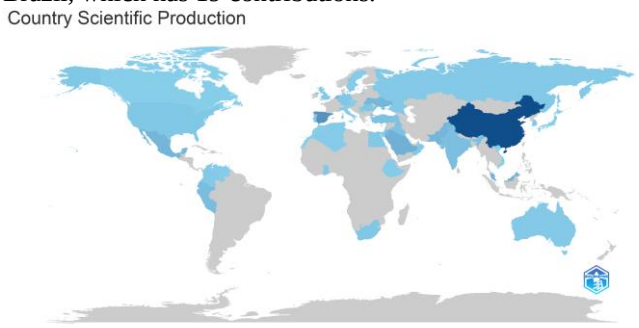

Fig. 4 Country Scientific Production.

Regarding the publications found in the study in Fig. 3, the most outstanding sources can be distinguished. In this case, the most relevant source is the journal "IEEE ACCESS" with 24 publications representing 34.29% of the total, followed by "Sensors" and "IEEE Transactions on Industrial Informatics" with 14 and 7 respectively. These results show the influence of these journals in the dissemination of key research in the field of technology and industrial informatics.

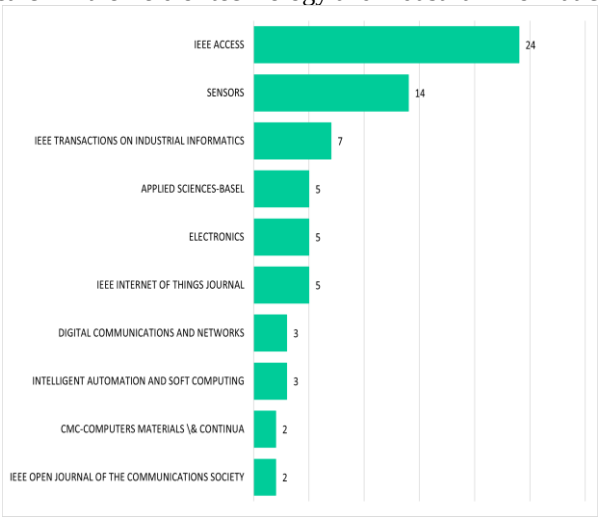

Fig. 5 Bibliometric evaluation based on the number of publications per scientific journal.

Fig. 6 shows a trend of words that were used by the authors in their articles. The words with the largest dimension are the most frequent. For example, "Industrial internet of things" with the light blue tone is repeated 37 times among the most used words. Followed by "Iiot" and "Security" with the golden and purple tone respectively are repeated 28 times. On the other hand, "Industry 4.0" with the light blue tone was repeated 24 times, also the terms such as "Blockchain" and "Industry 4" with orange and purple colors are repeated 22 times each.

Fig. 6 Visualization of the keyword thematic network.

Regarding the following Fig. 7, it shows us the number of countries with corresponding authors and their participation in scientific publications. Where they are separated by two sectors: Single Country Publications (SCP, in blue) and Multi-Country Publications (MCP, in red). Here we can see how China leads the scientific production with the largest number of research, but MCP stands out, followed by India, where the same happens as China, where the largest amount of MCP is produced. On the other hand, Spain has a higher production of SCP. In addition, countries such as "Canada", "Ireland", "Romania" and "Italy" are countries with only SCP production. The leading country in South America is "Brazil" where there is a combination of SCP and CCM, where the latter leads in Brazil, which indicates that they have a strong capacity to produce at the national level.

B. Content findings

In the systematic review conducted, it was identified that Blockchain stands out as a predominant tool to improve security in Industry 4.0. Of the 12 studies analyzed, its implementation is mainly oriented to provide an additional layer of security in transactions [23], guaranteeing data integrity and preventing unauthorized manipulations [24], [25]. For example, the use of authentication proofs ensures the reliability of industrial systems, while optimizing energy efficiency in these environments [26].

In addition, Blockchain is also key to establishing a trusted environment for data management, ensuring privacy in the storage, reception and exchange of information [27]. This is achieved through cryptography applied to encrypted images and the implementation of IPFS systems, which mitigate problems of centralization and failures in traditional platforms [28], [29], [30]. Another outstanding advantage is its ability to train local learning models, which contributes to the decentralization of data processing [31]. Additionally, Blockchain allows the use of dynamic accumulators, thus reducing storage and communication overhead in the network [32]. This technology also facilitates the creation of a trust system through device authentication, optimizing security between interconnected nodes [33], [34].

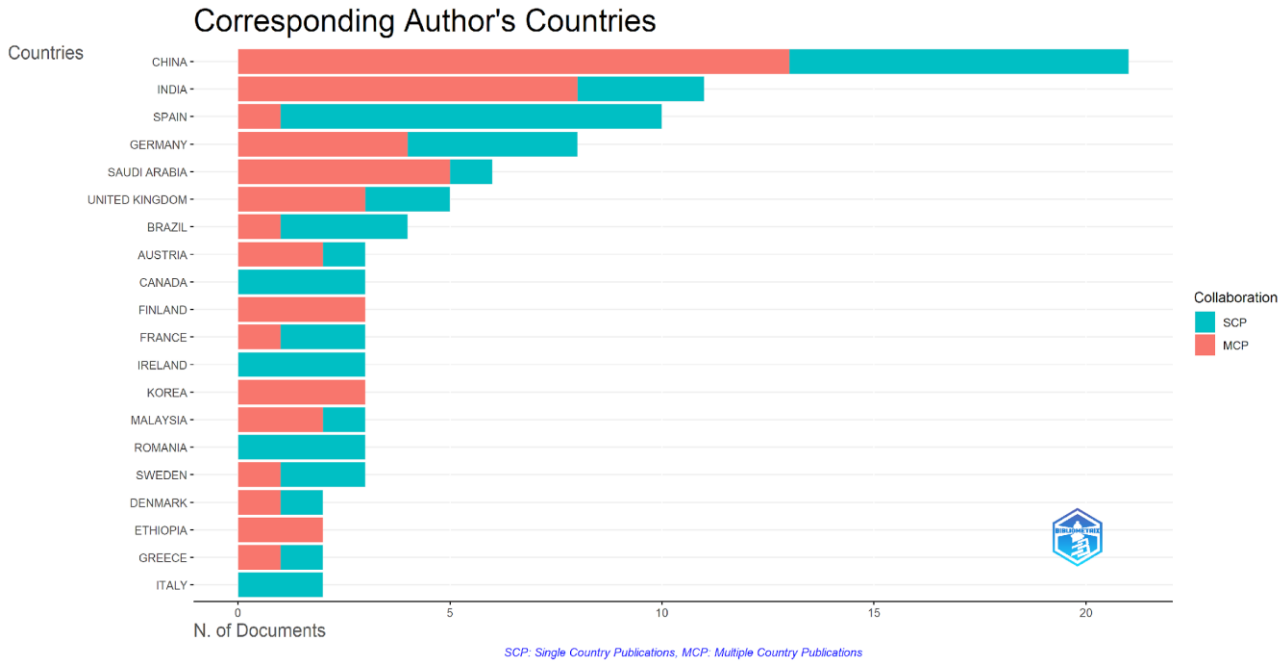

Fig. 7 Distribution of scientific publications by country

On the other hand, Machine Learning (ML) is used as an effective tool for the analysis of behavioral patterns, facilitating the detection of anomalies [24], [35], [36] and the consequent optimization of processes [37]. ML implements protection models by using genetic algorithms [26] and techniques such as the k-Nearest Neighbors (k-NN) algorithm, which detects threats based on the closeness of characteristics of potential intruders by comparing them with historical records of previous intrusions. This technique allows identifying similarities with previous security incidents, which facilitates early detection and more effective response to new threats [38]. In addition, tree algorithms have been employed in Multi-access Edge Computing (MEC) environments to reduce costs and improve operational efficiency [39], which reinforces the ability of ML to contribute to security and industrial performance.

Also, it was observed that Deep Learning (DL) tools are used for intrusion detection and classification [25]. This machine learning approach allows models to learn how to optimally allocate resources through a trial-and-error process [40]. DL models are capable of handling large volumes of data and extracting complex patterns, which is particularly useful for detecting hidden threats in large and complex data streams [35].

In addition, the Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) tool stands out, which acts as a protocol to secure end-to-end communication between IIoT devices [41]. These tools encrypt data transmitted over the network, ensuring protection against unauthorized access and tampering [42]. Of relevance is DTLS, as it is designed to operate over datagrams (UDP), a preferred transport protocol in many industrial systems due to its low latency [43].

In turn, Elliptic Curve Cryptography (ECC) and Convolutional Neural Networks (CNN) tools play a crucial role in industrial cybersecurity. ECC is a resource-efficient algorithm based on complex mathematical problems, such as the discrete logarithm problem on elliptic curves, which makes it extremely difficult for attackers to decrypt information [44]. This efficiency makes it particularly suitable for IoT devices with power and storage constraints [45]. In this context, ECC is used to generate the public and private keys needed for encryption and authentication in Blockchain networks. On the other hand, CNNs are employed to analyze large volumes of traffic in IoT networks, identifying patterns in network characteristics that may be associated with malicious activities, such as those carried out by botnets like Mirai and Gafgyt [46].

Similarly, it is important to consider Long Short-Term Memory (LSTM) and Software Defined Networking (SDN) tools. LSTM uses machine learning to analyze network data, helping to identify attacks in IIoT networks by detecting changes in traffic over time, such as sudden spikes or denial-of-service (DoS) attempts [46]. On the other hand, SDN separates data control and forwarding functions, allowing centralized network management [47]. This facilitates greater security and privacy in 5G-enabled environments, as it allows segmenting and isolating network traffic, which is crucial to mitigate attacks and protect data [24].

Table “IV” also presents the Intrusion Detection Systems (IDS) tool, whose main contribution lies in monitoring and detecting anomalies within network systems. IDSs

continuously monitor network traffic, analyzing data in search of anomalous behavior or predefined attack patterns. This constant monitoring not only makes it possible to identify possible threats but also facilitates a rapid response to possible cyber-attacks in real time, improving the ability of organizations to react to security incidents, which is essential in industrial environments where data availability and protection are critical. In examining the tools applied within IIoT systems, their value lies not only in their ability to detect threats or preserve data privacy, but also in how they influence system performance. A more useful analysis comes from linking each tool to concrete indicators such as the rate of false alarms, detection speed, bandwidth usage, or energy consumption. For example, while some machine learning models are highly accurate in spotting irregularities, they can also demand more processing power, which may reduce efficiency. On the other hand, certain lightweight encryption methods may not be as advanced but often strike a better balance between speed and protection. Understanding these trade-offs helps industries choose the right tools based on their technical needs and cybersecurity goals.

TABLE IV
TOOLS COMPILED IN THE SYSTEMATIC REVIEW ON IIOT AND THEIR IMPACT ON INDUSTRY 4.0 CYBERSECURITY.

Tools	N° of Tools
Blockchain	12
ML (Machine Learning)	7
DP (Deep Learning)	3
TLS/DTLS (Transport Layer Security/DatagramTDS)	3
ECC (Elliptic Curve Cryptography)	2
CNN (Convolutional Neural Networks)	2
LSTM (Long Short-Term Memory)	2
SDN (Software Defined Networks)	2
IDS (Intrusion detection systems)	1

In this framework, several key issues influencing the impact of Industrial Internet of Things (IIoT) on cybersecurity within Industry 4.0 have been identified in Table “V”, where a systematic literature review will be conducted.

First, 20 studies were collected within which, IIoT contributes significantly in improving cybersecurity performance in Industry 4.0, through a blockchain-based security framework it was observed that in the cement industry it solved the 51% security problem and Sybil attacks caused by existing consensus algorithms [26], in addition to great improvements in scheduling and latency analysis, with 30% and 23% reduction in latency using methods such as Q-learning and DDPG, respectively [26].

To this extent, a prototype of the monitoring framework was presented to ensure that IIoT devices comply with security standards as this helps prevent attacks such as denial of service (DoS), malware, and unauthorized access [48]. The latency in the IPFS network was significantly lower, and the system achieved a throughput of up to 110 transactions per second (TPS) [29], on the other hand, the IPFS-based system proved to be faster than traditional TCP/IP networks, especially for small files (e.g., 5 MB files were transferred almost four times faster) [29].

Subsequently, a performance analysis was performed where it showed that MAKE-IT is more efficient in terms of energy consumption and communication compared to other traditional schemes [42]. Under the same importance, encryption and authentication processes added minimal delay (around 1 second) due to TPM operations, which was acceptable according to the case constraints [41], meanwhile in [24] it is mentioned that IIoT can improve energy efficiency by using technologies such as D2D (device-to-device) communication and load balancing.

After the combination of techniques, the system detected attacks quickly and efficiently, which is vital for real-time industrial systems [46]. On the other hand, simulation and performance evaluation reveal that SUSIC achieves a better balance between security functionalities and computational costs compared to other systems [47]. Also, when compared to other methods, BDL-PPDT stands out for its improvements in network throughput (99.71 Mbps with 100 IoT sensors), higher packet delivery rate (99.72%) and longer network lifetime (3633 rounds) [32].

In addition, IIoT improves computational and communication cost efficiency, with a total authentication time of 10,539 ms [44]. The proposed protocol also increases the computational cost efficiency by 22.67% and communication cost efficiency by 16.35% over other similar protocols [33]. Also, in experimental simulations, it showed higher resource utility and learning efficiency, indicating overall superior performance [31].

Also, the agents were trained to keep CPU and bandwidth usage below 80%, avoiding overloads [40], which is why there is the Hidra protocol that ensures protection against unauthorized access through policies [37] and the system demonstrating low power consumption and high efficiency in computational complexity making it suitable for IoT devices [45].

In essence, through the ANN model, 96% accuracy was achieved and improved access control flexibility [34], where PVC optimizes the use of storage space and reduces communication loss, crucial for blockchain-based IIoT security [44], improving interoperability and handling of large volumes of data and devices [23].

Secondly, 13 additional publications reveal the relationship of IIoT and attack detection accuracy, in [26] the model predicted with an accuracy of 95.1% in training and 94.5% in testing, with a saving of 28.10% in energy consumption. In addition, the following results obtained in the HGSODL-ID model are shown, where it has superior performance compared to other recent approaches, achieving a maximum accuracy of 99.43% [49].

Similarly, the hybrid CNN-LSTM model achieved 99% accuracy in attack detection, outperforming other models such as CNN (92.9%) and WDLSTM (96.7%) [50], likewise, in [36] shows high performance in attack detection even with limited labeled data. On the other hand, in [51] students

learned accurately to detect attacks, obtaining that 13% of the analyzed IIoT/Industry 4.0 systems could be easily accessed due to poor security configurations.

Accordingly, the proposed system uses IIoT to monitor and analyze industrial network traffic, improve intrusion detection and classify traffic using CCSOA algorithm and OWKELM method [38], in [25] experimental results indicated that the PPBDL-IIoT approach achieved an accuracy of 91. 50% in detecting intrusions with the ICSCA dataset, likewise the combination of CNN and LSTM achieved 99.95% accuracy in identifying botnet attacks in the IIoT environment, demonstrating the effectiveness of this hybrid architecture [46].

In addition, research in [35] demonstrates high recall rates and accuracy, with a focus on reducing false positives and improving detection speed, achieving an accuracy of 99.99% in intrusion detection using algorithms such as XGBoost on the BoT-IoT dataset. In [32], an accuracy of 98.15% in intrusion detection is reported, in turn, the GJODL-CADC method showed significant improvements in the detection and classification of cyber-attacks, achieving an accuracy of 99.45% in the UNSWNB15 dataset and 98.52% in the UCI SECOM dataset [52].

In summary, the proposed threat detector, evaluated in a test environment for IIoT in [39], shows an average efficiency between 95% and 99% in the F1 Score metric, suggesting its feasibility for these scenarios, similarly, the federated and handoff approach applied to low-capacity devices achieve an accuracy above 99% in intrusion detection using the KDD99 dataset [27].

Finally, the data privacy protection obtained from IIoT has been evidenced through 8 studies. In this framework, the method of [28] achieved an NPCR of up to 99.57%, indicating higher security against small changes in encrypted data, where the protocol guarantees data confidentiality by using symmetric and asymmetric cryptography, protecting the identity of users and preventing unauthorized access [42].

End-to-end encryption ensures the confidentiality and integrity of exchanged data, as demonstrated in a predictive maintenance scenario in the railway industry, where the developed prototype succeeded in rejecting forged messages and malicious gateways during secure communication tests [41]. In addition, the work in [24] describes a framework for privacy protection in 5G-enabled communications using algorithms and mathematical models to ensure data security.

Also, SUSIC is considered secure against several known cyber threats, such as man-in-the-middle attacks, spoofing attacks, and ephemeral secret leaks [47] and thus is used to secure data between IT and OT systems, preventing unauthorized access or modification [53].

This is why the use of lightweight protocols and algorithms allows improving security without compromising performance in complex and distributed industrial networks [43], where access control is implemented to ensure that only authenticated devices can participate in communications, preventing attacks such as spoofing and unauthorized access [53].

To succeed, a business needs to improve efficiency and adapt to the market. By using resources effectively, cutting costs, and increasing production, companies can improve quality and satisfy customers. This helps create a competitive edge and strengthen internal processes.

TABLE V
EFFECTS COMPILED IN THE SYSTEMATIC REVIEW ON IIOT AND ITS IMPACT ON INDUSTRY 4.0 CYBERSECURITY.

Aspects and effects found	N° of Effects
Security	**41**
Improved performance	20
Accurate attack detection	13
Data privacy protection	8
Total	**41**

III. CONCLUSIONS

The implementation of the Industrial Internet of Things (IIoT) in Industry 4.0 has driven significant advances in operational efficiency but has also generated cybersecurity challenges that require specialized attention. This systematic review has identified key technologies such as Blockchain, Machine Learning, Deep Learning and Intrusion Detection Systems (IDS), which play a crucial role in protecting industrial systems. These tools not only improve data integrity and confidentiality but also optimize intrusion detection and mitigate threats more effectively.

Among these technologies, Blockchain stands out for its ability to ensure data integrity and reduce latency in networks, improving both the security and performance of IIoT environments. In turn, Machine Learning and Deep Learning enable more accurate anomaly detection, which strengthens cybersecurity by identifying complex patterns in data traffic and preventing attacks in real time.

The review also highlights the importance of databases such as Web of Science (WoS), which has been instrumental in compiling relevant studies. Thanks to this source, a comprehensive analysis has been conducted that has identified key trends in IIoT cybersecurity research. The studies indicate that the field continues to evolve, with advances such as Blockchain-based cryptography and the use of convolutional neural networks, which are laying the groundwork for more robust security solutions.

However, significant challenges remain. Adoption of these technologies in countries with less research capacity remains limited, increasing risks in critical infrastructure protection. In addition, the lack of uniformity in the implementation of cybersecurity standards represents a considerable obstacle to achieving effective protection at a global level.

REFERENCES

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," IEEE Trans Industr Inform, vol. 14, no. 11, pp. 4724–4734, Nov. 2018, doi: 10.1109/TII.2018.2852491.

[2] M. B. Shishehgarkhaneh, R. C. Moehler, and S. F. Moradinia, "Blockchain in the Construction Industry between 2016 and 2022: A Review, Bibliometric, and Network Analysis," Smart Cities, vol. 6, no. 2, pp. 819–845, Mar. 2023, doi: 10.3390/SMARTCITIES6020040.

[3] A. M. Alnajim, S. Habib, M. Islam, S. M. Thwin, and F. Alotaibi, "A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things," Technologies (Basel), vol. 11, no. 6, pp. 1–26, Dec. 2023, doi: 10.3390/technologies11060161.

[4] L. Borgosz and D. Dikicioglu, "Industrial internet of things: What does it mean for the bioprocess industries?," Biochem Eng J, vol. 201, pp. 1–11, Jan. 2024, doi: 10.1016/j.bej.2023.109122.

[5] A. Anagnostopoulou, I. Mavridis, and D. Gritzalis, "Risk-Based Illegal Information Flow Detection in the IIoT," Proceedings of the International Conference on Security and Cryptography, vol. 1, pp. 377–384, Jan. 2023, doi: 10.5220/0012079800003555.

[6] B. Alotaibi, "A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities," Sensors, vol. 23, no. 17, pp. 1–49, Sep. 2023, doi: 10.3390/s23177470.

[7] S. Pal and Z. Jadidi, "Analysis of security issues and countermeasures for the industrial internet of things," Applied Sciences (Switzerland), vol. 11, no. 20, pp. 1–33, Oct. 2021, doi: 10.3390/app11209393.

[8] H. Ali, M. S. Khan, M. Driss, J. Ahmad, W. J. Buchanan, and N. Pitropakis, "CellSecure: Securing Image Data in Industrial Internet-of-Things via Cellular Automata and Chaos-Based Encryption," IEEE Vehicular Technology Conference, pp. 1–6, Oct. 2023, doi: 10.1109/VTC2023-Fall60731.2023.10333478.

[9] E. Lomba, R. Severino, and A. F. Vilas, "Work In Progress: Towards Adaptive RF Fingerprint-based Authentication of IIoT devices," IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, vol. 2022, pp. 1–4, Jan. 2022, doi: 10.1109/ETFA52439.2022.9921575.

[10] H. L. Hassani, A. Bahnasse, E. Martin, C. Roland, O. Bouattane, and M. El Mehdi Diouri, "Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443," Procedia Comput Sci, vol. 191, pp. 33–40, Jan. 2021, doi: 10.1016/j.procs.2021.07.008.

[11] F. A. B. Juarez, "Cybersecurity in an industrial internet of things environment (IIoT): Challenges for standards systems and evaluation models," 2019 8th International Conference on Software Process Improvement, CIMPS 2019 - Applications in Software Engineering, vol. 10, pp. 124747–124765, Oct. 2019, doi: 10.1109/CIMPS49236.2019.9082437.

[12] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," Institute of Electrical and Electronics Engineers, pp. 519–524, Jan. 2016, doi: 10.1109/ASPDAC.2016.7428064.

[13] F. Martin-Tricot, C. Eichler, and P. Berthome, "Secure key distribution in heterogeneous interoperable industrial Internet of Things," International Conference on Wireless and Mobile Computing, Networking and Communications, vol. 2021, pp. 74–79, Jan. 2021, doi: 10.1109/WiMob52687.2021.9606265.

[14] V. S. Magomadov, "The Industrial Internet of Things as one of the main drivers of Industry 4.0," IOP Conf Ser Mater Sci Eng, vol. 862, no. 3, pp. 1–4, May 2020, doi: 10.1088/1757-899X/862/3/032101.

[15] G. S. Miñan, J. A. Moreno, and X. D. Fernández, "LIA Method for the Application of Microsoft Excel in Data Tabulation in Systematic Reviews," CEUR Workshop Proc, vol. 3691, 2023, Accessed: Jun. 14, 2024. [Online]. Available: https://ceur-ws.org/Vol-3691/paper3.pdf

[16] R. Bravo Toledo, "La declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas," PLoS Med, 2021, Accessed: Aug. 05, 2023. [Online]. Available: https://ccamposhugf.files.wordpress.com/2021/04/prisma_2020_statement_definitivo-espanol-completo.pdf

[17] M. J. Page et al., "A declaração PRISMA 2020: diretriz atualizada para relatar revisões sistemáticas," Revista Panamericana de Salud Publica/Pan American Journal of Public Health, vol. 46, 2022, doi: 10.26633/RPSP.2022.112.

[18] Hutton, F. Catalá-López, and D. Moher, "La extensión de la declaración PRISMA para revisiones sistemáticas que incorporan metaanálisis en red: PRISMA-NMA," Med Clin (Barc), vol. 147, no. 6, pp. 262–266, Sep. 2016, doi: 10.1016/J.MEDCLI.2016.02.025.

[19] Moher et al., "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement," Syst Rev, vol. 4, no. 1, pp. 148–160, 2016, doi: 10.1186/2046-4053-4-1.

[20] G. Urrútia and X. Bonfill, "Declaración PRISMA: una propuesta para mejorar la publicación de revisiones sistemáticas y metanálisis," Med Clin (Barc), vol. 135, no. 11, pp. 1–5, Sep. 2010, doi: 10.1016/J.RECESP.2021.06.016.

[21] S. Briscoe, "Errors to avoid when searching for studies for systematic reviews: A guide for nurse researchers," Int J Older People Nurs, vol. 18, no. 3, May 2023, doi: 10.1111/OPN.12533.

[22] G. Urrutia and X. Bonfill, "Revisiones sistemáticas: una herramienta clave para la toma de decisiones clínicas y sanitarias," Rev Esp Salud Publica, vol. 88, no. 1, pp. 1–3, 2014, doi: 10.4321/S1135-57272014000100001.

[23] Y. Wu, H. N. Dai, and H. Wang, "Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0," IEEE Internet Things J, vol. 8, no. 4, pp. 2300–2317, Feb. 2021, doi: 10.1109/JIOT.2020.3025916.

[24] M. Humayun, N. Z. Jhanjhi, M. Alruwaili, S. S. Amalathas, V. Balasubramanian, and B. Selvaraj, "Privacy protection and energy optimization for 5G-aided industrial internet of things," IEEE Access, vol. 8, pp. 183665–183677, Jan. 2020, doi: 10.1109/ACCESS.2020.3028764.

[25] A. M. Hilal et al., "Intelligent Deep Learning Model for Privacy Preserving IIoT on 6G Environment," Computers, Materials and Continua, vol. 72, no. 1, pp. 333–348, Jan. 2022, doi: 10.32604/cmc.2022.024794.

[26] S. F. Ahmed et al., "Industrial Internet of Things enabled technologies, challenges, and future directions," Computers and Electrical Engineering, vol. 110, pp. 1–16, Sep. 2023, doi: 10.1016/j.compeleceng.2023.108847.

[27] P. Zhang, H. Sun, J. Situ, C. Jiang, and D. Xie, "Federated Transfer Learning for IIoT Devices with Low Computing Power Based on Blockchain and Edge Computing," IEEE Access, vol. 9, pp. 98630–98638, Jan. 2021, doi: 10.1109/ACCESS.2021.3095078.

[28] R. Bhaskaran, R. Karuppathal, M. Karthick, J. Vijayalakshmi, S. Kadry, and Y. Nam, "Blockchain Enabled Optimal Lightweight Cryptography Based Image Encryption Technique for IIoT," Intelligent Automation and Soft Computing, vol. 33, no. 3, pp. 1593–1606, Jan. 2022, doi: 10.32604/iasc.2022.024902.

[29] Chen, J. Yang, W.-J. Tsaur, W. Weng, C. Wu, and X. Wei, "Enterprise Data Sharing with Privacy-Preserved Based on Hyperledger Fabric Blockchain in IIOT's Application," Sensors, vol. 22, no. 3, pp. 1–23, Feb. 2022, doi: 10.3390/s22031146.

[30] J. Wang, G. Huang, R. Simon Sherratt, D. Huang, and J. Ni, "Data secure storagemechanism for IIoT based on blockchain," Computers, Materials and Continua, vol. 78, no. 3, pp. 4029–4048, Jan. 2024, doi: 10.32604/cmc.2024.047468.

[31] C. Qiu, G. S. Aujla, J. Jiang, W. Wen, and P. Zhang, "Rendering Secure and Trustworthy Edge Intelligence in 5G-Enabled IIoT Using Proof of Learning Consensus Protocol," IEEE Trans Industr Inform, vol. 19, no. 1, pp. 900–909, Jan. 2023, doi: 10.1109/TII.2022.3179272.

[32] K. Lakshmanna, R. Kavitha, B. T. Geetha, A. K. Nanda, A. Radhakrishnan, and R. Kohar, "Deep Learning-Based Privacy-Preserving Data Transmission Scheme for Clustered IIoT Environment," Comput Intell Neurosci, vol. 2022, pp. 1–11, Jan. 2022, doi: 10.1155/2022/8927830.

[33] K. Mahmood et al., "Blockchain and PUF-based secure key establishment protocol for cross-domain digital twins in industrial Internet of Things architecture," J Adv Res, vol. 62, pp. 155–163, Aug. 2024, doi: 10.1016/j.jare.2023.09.017.

[34] M. Usman, M. S. Sarfraz, U. Habib, M. U. Aftab, and S. Javed, "Automatic Hybrid Access Control in SCADA-Enabled IIoT Networks

Using Machine Learning," Sensors, vol. 23, no. 8, pp. 1–21, Apr. 2023, doi: 10.3390/s23083931.
[35] L. Idouglid, S. Tkatek, K. Elfayq, and A. Guezzaz, "Next-gen security in IIoT: integrating intrusion detection systems with machine learning for industry 4.0 resilience," International Journal of Electrical and Computer Engineering, vol. 14, no. 3, pp. 3512–3521, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3512-3521.
[36] O. Aouedi, K. Piamrat, G. Muller, and K. Singh, "Federated Semisupervised Learning for Attack Detection in Industrial Internet of Things," IEEE Trans Industr Inform, vol. 19, no. 1, pp. 286–295, Jan. 2023, doi: 10.1109/TII.2022.3156642.
[37] J. Sasiain, A. Sanz, J. Astorga, and E. Jacob, "Towards flexible integration of 5G and IIoT technologies in industry 4.0: A practical use case," Applied Sciences (Switzerland), vol. 10, no. 21, pp. 1–20, Nov. 2020, doi: 10.3390/app10217670.
[38] R. Gopi et al., "Intelligent Intrusion Detection System for Industrial Internet of Things Environment," Computer Systems Science and Engineering, vol. 44, no. 2, pp. 1567–1582, Jan. 2023, doi: 10.32604/csse.2023.025216.
[39] S. Ruiz-Villafranca, J. Roldán-Gómez, J. Carrillo-Mondéjar, J. M. C. Gómez, and J. M. Villalón, "A MEC-IIoT intelligent threat detector based on machine learning boosted tree algorithms," Computer Networks, vol. 233, pp. 1–15, Sep. 2023, doi: 10.1016/j.comnet.2023.109868.
[40] J. Rosenberger et al., "Deep Reinforcement Learning Multi-Agent System for Resource Allocation in Industrial Internet of Things," Sensors, vol. 22, no. 11, pp. 1–23, Jun. 2022, doi: 10.3390/s22114099.
[41] O. Gilles, D. Gracia Pérez, P. A. Brameret, and V. Lacroix, "Securing IIoT communications using OPC UA PubSub and Trusted Platform Modules," Journal of Systems Architecture, vol. 134, pp. 1–13, Jan. 2023, doi: 10.1016/j.sysarc.2022.102797.
[42] K. Choudhary, G. S. Gaba, I. Butun, and P. Kumar, "Make-it—a lightweight mutual authentication and key exchange protocol for industrial internet of things," Sensors (Switzerland), vol. 20, no. 18, pp. 1–21, Jan. 2020, doi: 10.3390/s20185166.
[43] A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, and A. Urbieta, "Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0," J Manuf Syst, vol. 57, pp. 367–378, Oct. 2020, doi: 10.1016/j.jmsy.2020.10.011.
[44] N. Li, M. Ma, and H. Wang, "ASAP-IIOT: An Anonymous Secure Authentication Protocol for Industrial Internet of Things," Sensors, vol. 24, no. 4, pp. 1–23, Feb. 2024, doi: 10.3390/s24041243.
[45] S. M. Umran, S. Lu, Z. A. Abduljabbar, J. Zhu, and J. Wu, "Secure data of industrial internet of things in a cement factory based on a blockchain technology," Applied Sciences (Switzerland), vol. 11, no. 14, pp. 1–16, Jul. 2021, doi: 10.3390/app11146376.
[46] Z. Hussain, A. Akhunzada, J. Iqbal, I. Bibi, and A. Gani, "Secure IIoT-enabled industry 4.0," Sustainability (Switzerland), vol. 13, no. 22, pp. 1–14, Nov. 2021, doi: 10.3390/su132212384.
[47] A. Irshad, G. A. Mallah, M. Bilal, S. A. Chaudhry, M. Shafiq, and H. Song, "SUSIC: A Secure User Access Control Mechanism for SDN-Enabled IIoT and Cyber-Physical Systems," IEEE Internet Things J, vol. 10, no. 18, pp. 16504–16515, Sep. 2023, doi: 10.1109/JIOT.2023.3268474.
[48] Bicaku, M. Tauber, and J. Delsing, "Security standard compliance and continuous verification for Industrial Internet of Things," Int J Distrib Sens Netw, vol. 16, no. 6, pp. 1–19, Jun. 2020, doi: 10.1177/1550147720922731.
[49] K. M. Alalayah et al., "Optimal Deep Learning Based Intruder Identification in Industrial Internet of Things Environment," Computer Systems Science and Engineering, vol. 46, no. 3, pp. 3121–3139, Jan. 2023, doi: 10.32604/csse.2023.036352.
[50] Ankita, S. Rani, A. Singh, D. H. Elkamchouchi, and I. D. Noya, "Lightweight Hybrid Deep Learning Architecture and Model for Security in IIOT," Applied Sciences (Switzerland), vol. 12, no. 13, pp. 1–11, Jul. 2022, doi: 10.3390/app12136442.
[51] T. M. Fernández-Caramés and P. Fraga-Lamas, "Use case based blended teaching of IIoT cybersecurity in the industry 4.0 era," Applied Sciences (Switzerland), vol. 10, no. 16, pp. 1–29, Aug. 2020, doi: 10.3390/app10165607.
[52] L. A. Maghrabi, I. R. Alzahrani, D. Alsalman, Z. M. AlKubaisy, D. Hamed, and M. Ragab, "Golden Jackal Optimization with a Deep Learning-Based Cybersecurity Solution in Industrial Internet of Things Systems," Electronics (Switzerland), vol. 12, no. 19, pp. 1–17, Oct. 2023, doi: 10.3390/electronics12194091.
[53] S. Mantravadi, R. Schnyder, C. Møller, and T. D. Brunoe, "Securing IT/oT links for low power IIoT devices: Design considerations for industry 4.0," IEEE Access, vol. 8, pp. 200305–200321, Jan. 2020, doi: 10.1109/ACCESS.2020.3035963.
[54] Vijayakumaran, B. Muthusenthil, and B. Manickavasagam, "A reliable next generation cyber security architecture for industrial internet of things environment," International Journal of Electrical and Computer Engineering, vol. 10, no. 1, pp. 387–395, Jan. 2020, doi: 10.11591/ijece.v10i1.pp387-395.