ISSN 2007-9737

Impact of Artificial Intelligence on Cyberattack Detection: A Systematic Review of Recent Studies

Brayan Puma-Sosa[1], Jhafet Atachagua-Bernuy[1], Fabrizio Del Carpio Delgado[2], Mario Rodriguez Vasquez[2], Germán Machicado Lea[2], Ángel Núñez Meza[3], Javier Gamboa-Cruzado[4], Ivar Farfán Muñoz[4], Germán Rios-Toledo[5,*]

[1] Universidad Nacional Federico Villarreal, Peru

[2] Universidad Nacional de Moquegua, Peru

[3] Universidad Nacional Daniel Alcides Carrión, Peru

[4] Universidad Nacional Mayor de San Marcos, Peru

[5] Tecnológico Nacional de México/Instituto Tecnológico de Tuxtla Gutierrez, Mexico

{2022016612, 2021018265}@unfv.edu.pe, {fdelcarpiod, mrodriguezv, gmachicadol }@unam.edu.pe, anunezm@undac.edu.pe, {jgamboac, ifarfanm}@unmsm.edu.pe, german.rt@tuxtla.tecnm.mx

Abstract The increasing sophistication of cyberattacks has exposed the limitations of traditional detection mechanisms and encouraged the use of artificial intelligence to develop more adaptive solutions. This study aims to analyze the current state of scientific knowledge concerning the application of artificial intelligence to cyberattack detection by integrating technological, evaluative, conceptual, collaborative, and thematic perspectives. A systematic literature review complemented by bibliometric analysis was conducted through searches of IEEE Xplore, Scopus, Web of Science, SpringerLink, and the ACM Digital Library. The PRISMA approach, exclusion criteria, and quality assessment were applied, yielding 61 studies for the final synthesis. The results show a marked concentration of Python and Scala as programming environments, while Detection Rate and False Positive Rate predominate as evaluation criteria. Conceptual definitions primarily address technical and functional dimensions, whereas applied approaches remain less developed. Scientific collaboration also displays prominent bridging nodes, and the thematic structure combines specialized areas, such as IoT Security and Intrusion Detection, with research lines that remain insufficiently consolidated. In conclusion, the field is progressing toward greater specialization, although asymmetries persist among technical performance, evaluation, conceptualization, scientific cooperation, and thematic maturity.

Keywords. Machine learning, deep learning, intrusion detection, hybrid systems, detection accuracy, bibliometric review.

1 Introduction

Cybersecurity has become a global concern due to the growing number and sophistication of threats such as phishing, ransomware, and intrusions into information systems. These conditions reveal the limitations of traditional signature-based detection systems when confronted with unknown and dynamic attacks. In this context, artificial intelligence offers predictive and classification capabilities that can strengthen cyberattack detection; however, challenges persist regarding false positives, model interpretability, and adaptation to changing environments.

In the field of intelligent intrusion detection, various studies have oriented their efforts towards the development of more robust systems through

machine learning, hybrid architectures and models that combine neural networks with decision methods, demonstrating an evolution from conventional approaches to detection mechanisms with greater adaptive capacity [2, 3, 12]. Research focused on IoT environments has proposed distributed and adaptive architectures based on deep learning, Lambda architecture and processing at fog or edge nodes, with the purpose of improving the scalability and efficiency of intrusion detection systems [4, 21, 24].

Additionally, other studies have applied ensemble and machine learning models in specific domains such as smart grids, the Internet of Medical Things, and wireless sensor networks, incorporating multiple classifiers, Stacking, Bagging, and Boosting techniques, as well as dimensionality reduction and context-awareness mechanisms [7, 8, 48]. From an operational perspective, researchers have also examined the incorporation of artificial intelligence to increase the efficiency of Security Operations Centers and, in parallel, the use of statistical feature-selection procedures to improve the performance of classifiers employed in intrusion detection [16, 22]. Another relevant research stream integrates optimization techniques with artificial intelligence, combining deep learning with metaheuristic methods, reinforcement learning, and Bayesian optimization to strengthen threat identification and detection-system performance [11, 26, 30].

Regarding the modeling of complex dependencies, hybrid architectures have been proposed that combine ConvLSTM-Seq2Seq, LSTM and Auto-Encoders, allowing to represent spatial and temporal relationships associated with the behavior of network traffic [18, 19]. In the same line of hybridization, other studies have developed self-adaptive systems that articulate signature-based detection mechanisms with LSTM-supported anomaly detection models and deep learning, seeking to take advantage of the complementary strengths of both approaches [28, 31]. It is also worth highlighting proposals aimed directly at improving the discriminatory capacity of IDS through attention mechanisms, treatment of traffic imbalance and combination of methods of feature selection with stacking classifiers; in the latter case, an F1-score of 96% was reported on CICDDoS-2019 [29, 32, 34]. Another clearly identifiable trend corresponds to the optimization of the input representations and the classification process, through feature selection, dimensionality reduction and advanced classification techniques, strategies recurrently used to strengthen the detection of sophisticated attacks [36, 38, 43]. Relatedly, hybrid methods and advanced systems have been proposed that combine feature selection, anomaly detection, machine learning and data optimization with the aim of increasing the accuracy of detection mechanisms [35, 37, 42].

In smart-grid scenarios, research has also integrated deep learning models with optimization methods, producing approaches intended to improve the performance of security systems against emerging threats [39,45]. Finally, studies that examine the application of artificial intelligence and deep learning to attack detection more broadly are consistent with reviews focused on anomaly-detection techniques in IoT ecosystems, highlighting the relevance of these approaches to unknown threats [40, 68].

Reference [67] analyzes artificial intelligence-based cyberattacks in the context of Industry 4.0, identifying their risks and evolution. Reference [70] presents a systematic review of ensemble machine learning-based intrusion detection systems (IDS), examining current methods, datasets, and trends. Reference [71] provides an in-depth review of deep learning-based IDS and classifies the methods according to the techniques employed. Finally, [72] conducts a systematic review of deep learning techniques applied to network intrusion detection systems (NIDS), following the PRISMA 2020 guidelines, and analyzes advances in architectures, metrics, tools, and emerging cybersecurity trends. In other contexts, machine learning has also been applied to other text-analysis domains, such as sentiment analysis of Twitter communications using Support Vector Machine [91], demonstrating the versatility of these techniques beyond cyberattack detection, which is the focus of the present study.

The existing literature has addressed Artificial Intelligence applied to cybersecurity from specific perspectives, such as Industry 4.0, intrusion detection systems, ensemble learning and deep learning. However, an integration gap persists, as these studies analyze particular dimensions without providing a joint characterization of the

technologies used, evaluation criteria, quality of publications, conceptual approaches, cross-country collaboration and thematic trends.

Consequently, it is necessary to develop a systematic review complemented by bibliometric analysis that integrates these dimensions and provides a more structured view of the current state of Artificial Intelligence applied to Cyberattack Detection.

The growing application of Artificial Intelligence in Cyberattack Detection has generated a broad scientific production, although fragmented in technological approaches, evaluation metrics, application contexts and specific thematic lines.

In this scenario, it is necessary to systematically integrate the available evidence to understand how this field is structured and evolved, identifying the technologies used, the criteria used to evaluate the performance, the quality of the publications, the main conceptual approaches, the patterns of collaboration between countries and the predominant thematic trends.

Consequently, the main objective is to analyze the current state of scientific knowledge about the application of Artificial Intelligence in the Detection of Cyberattacks through a systematic review of the literature complemented by bibliometric analysis, with the purpose of characterizing their technological and methodological approaches, examining their patterns of production and scientific collaboration and identifying trends and emerging areas of research.

The work is organized as follows: Section 2, Background, presents the background and conceptual foundations that contextualize the application of Artificial Intelligence in the Detection of Cyberattacks, considering the increasing frequency and sophistication of threats and the limitations of traditional approaches. Section 3, Research Methodology, describes the procedure followed to develop systematic literature review and bibliometric analysis. Section 4, Results and Discussion, presents, analyzes and interprets the main findings obtained based on the research questions raised. Finally, Section 5, Conclusions and Future Research, synthesizes the most relevant results, exposes the main implications of the study and proposes lines for further research.

2 Background

This systematic review of the literature (SLR) performs a comprehensive analysis of various scientific papers, establishing the necessary background and evidence to contextualize and base the object of study of this research.

2.1 Artificial Intelligence

Machine learning models aimed at detecting intrusions into the Internet of Medical Things were evaluated, highlighting the use of ensemble algorithms such as Stacking, Bagging and Boosting [8]. Another study examined the integration of Artificial Intelligence with Artificial Immune Systems (AIS) to increase the efficiency of Security Operations Centers (SOCs) [16]. An approach was also proposed that combines feature selection, dimensionality reduction and advanced classification, strengthening detection against sophisticated attacks [38].

Finally, a model with tree-based selection and LOF detection was presented, reaching 99.89% accuracy in R2L (NSL-KDD) attacks, although it showed limitations in UNSW-NB15 [35]. Another work raised an approach to detect malicious SSL traffic using artificial intelligence, specifically LSTM autoencoders and convolutional neural networks (CNNs).

From the analysis of reconstructed SSL records, malicious flows were accurately identified in encrypted channels, overcoming the limitations of conventional inspections at the TCP/IP level [59]. An artificial intelligence-based intrusion detection system was also proposed, combining RBF neural networks with SVM algorithms [61].

Another study looked at intruder detection systems based on artificial intelligence for IoT devices, highlighting the effectiveness of Graph Neural Networks (GNN) for their high accuracy and speed of training [93]. Finally, Aparcana-Tasayco and Gamboa-Cruzado [65], in a systematic review on machine learning for software-defined network management, identified Support Vector Machine as the most used technique (14.4%), a predominance that is reaffirmed in anomaly detection tasks and intrusion detection systems; this is consistent with the prevalence of machine

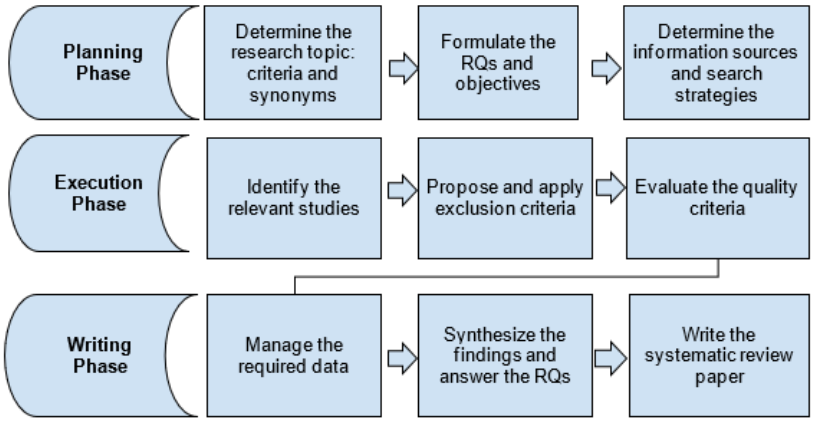

Fig. 1. Stages used in the SLR

learning approaches and hybrid systems observed in the detection of cyberattacks.

2.2 Detection of Cyberattacks

The paper proposes a distributed framework for the detection of cyberattacks in IoT networks, based on deep learning models. The solution increases the efficiency of the IDS by transferring the detection capabilities to the fog nodes, reaching high levels of accuracy and robustness in real scenarios [21]. Another study addresses the detection of attacks in networks using artificial intelligence and deep learning techniques. It proposes an innovative approach that integrates feature selection, dimensionality reduction and advanced classification, notably improving the capacity of intrusion detection systems against sophisticated attacks [36]. It also proposes an advanced system for the detection of network intrusions, whose approach combines machine learning and data optimization techniques to increase the accuracy of cyberattack identification, reduce false positive rates and improve overall system efficiency [37].

Similarly, another paper addresses network attack detection using artificial intelligence and deep learning methods, proposing an approach that combines feature selection, dimensionality reduction, and advanced classification to strengthen the capability of sophisticated attack intrusion detection systems [38]. Finally, a comprehensive approach is developed to detect attacks on smart grids by integrating deep learning models and optimization methods, obtaining significant improvements in the performance of network security systems and ensuring more effective detection of emerging threats under highly dynamic operating conditions [39].

2.3 From Artificial Intelligence to Adaptive Cyber Defense: Smart Detection Mechanisms Against Emerging Threats

Artificial intelligence has transformed cyberattack detection by replacing static rules with machine learning and deep learning models capable of learning traffic patterns, extracting discriminative features, and classifying anomalies in real time. Theoretically grounded in statistical learning, information theory, and pattern recognition, these mechanisms enable intrusion detection systems (IDS) to anticipate zero-day threats and adapt to dynamic environments such as IoT and fog networks. Nevertheless, this integration faces persistent challenges, including class imbalance, adversarial machine learning, high computational cost, and limited interpretability, which constrain deployment in real-world scenarios and motivate progress toward more advanced paradigms, such as ensemble models, graph neural networks, and explainable artificial intelligence (XAI). These foundations and tensions shape the analytical framework systematically addressed in the following sections through the literature review and bibliometric analysis.

Table 1. Research questions and objectives

Research Question	Objective
RQG: What is the current state of scientific knowledge about Artificial Intelligence and its impact on Cyberattack Detection?	**OG:** Determine the state of the art of research on Artificial Intelligence and its application in the detection of cyberattacks, analyzing their evolution, predominant approaches and repercussions in the field of cybersecurity
RQ1: What programming languages are used for the development of AI-based solutions?	**O1:** Identify which programming languages are most effective in the development of Artificial Intelligence
RQ2: What criteria are used to evaluate the performance of Cyberattack Detection?	**O2**: To specify the criteria used to evaluate the detection of cyberattacks
RQ3: What are the quartile levels of journals that publish research on the effect of Artificial Intelligence on Cyberattack Detection?	**O3**: Classify scientific journals based on their quartile levels in which research on artificial intelligence and cyberattack detection has been published
RQ4: What conceptual definitions have been proposed in the studies on Artificial Intelligence applied to Cyberattack Detection?	**O4**: Collect and classify the definitions of artificial intelligence applied to the detection of cyberattacks used in the scientific literature
RQ5: Which countries have the highest frequency of co-occurrence in research on Artificial Intelligence applied to Cyberattack Detection?	**O5**: Investigate the countries that have the highest co-occurrence in studies on artificial intelligence and detection of cyberattacks
RQ6: What thematic categories predominate in the scientific production on Artificial Intelligence applied to Cyberattack Detection?	**O6**: Identify the predominant thematic categories in AI research and cyberattack detection

3 Research Methodology

This systematic literature review (SLR) was developed through a structured process of identification, selection and analysis of scientific papers, following the methodological guidelines established by Kitchenham & Charters [62] and complemented by the procedures proposed by Kitchenham & Brereton [63], which allow organizing in a rigorous and reproducible way the stages of search, evaluation and selection of the available scientific evidence.

To facilitate understanding of the applied methodological procedure, Figure 1 sequentially presents the steps and steps followed during the development of this research.

The methodological procedure includes a precise definition of the phases developed in this SLR, each aimed at ensuring greater rigor and quality in the selection of the analyzed papers. Likewise, the PRISMA-SCR diagram [64] was incorporated, which facilitates the structured and transparent visualization of the exclusion criteria applied previously.

3.1 Problems and Objectives of Research

The main purpose of this systematic review is to analyze the current state of scientific knowledge about the application of Artificial Intelligence (AI) in the Detection of Cyberattacks. The study seeks to identify predominant methodological approaches, emerging thematic trends, patterns of scientific collaboration, as well as bibliometric and qualitative characteristics of the most relevant publications in this field.

To achieve this purpose, Table 1 presents specific descriptive and analytical questions, together with concrete objectives that guide the review from methodological, thematic, and bibliometric perspectives. These questions enable a comprehensive examination of the available scientific literature, the identification of knowledge gaps, the recognition of relevant convergences, and the establishment of opportunities for future

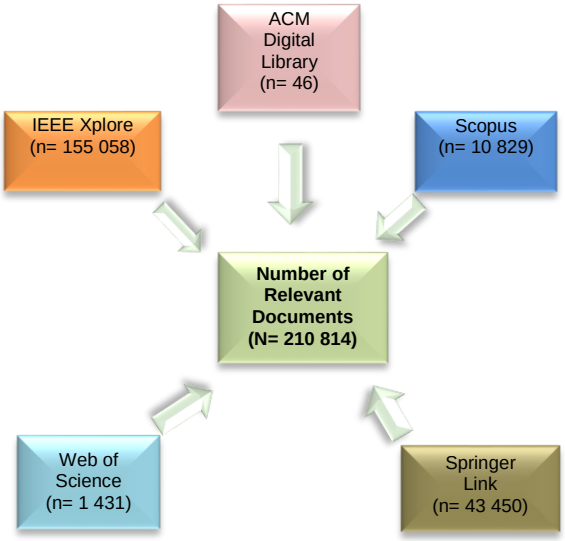

Fig. 2. Distribution of relevant documents by source of information

research on the interaction between AI and cybersecurity. The main purpose of this systematic review is to analyze the current state of scientific knowledge about the application of Artificial Intelligence (AI) in the Detection of Cyberattacks. The study seeks to identify predominant methodological approaches, emerging thematic trends, patterns of scientific collaboration, as well as bibliometric and qualitative characteristics of the most relevant publications in this field.

To achieve this purpose, Table 1 presents specific descriptive and analytical questions, together with concrete objectives that guide the review from methodological, thematic, and bibliometric perspectives. These questions enable a comprehensive examination of the available scientific literature, the identification of knowledge gaps, the recognition of relevant convergences, and the establishment of opportunities for future research on the interaction between AI and cybersecurity.

3.2 Sources of Information and Search Strategies

Systematic searches were carried out in scientific databases recognized for their quality, coverage and relevance: Scopus, Web of Science, IEEE Xplore, ACM Digital Library and Springer Link. To design the search strategies, descriptors classified by language and according to the variables of the study were defined, incorporating synonyms and terms related to the independent variable, Artificial Intelligence, and the dependent variable, Detection of Cyber Threats, in order to formulate more broad, precise and relevant search equations in each source consulted.

From these descriptors, specific search combinations were constructed, adapted to the syntax, structure and functionalities of each selected database; such combinations, together with the criteria used for their formulation, are presented in an organized and comparative manner in Table 2.

3.3 Identified Studies

At the initial stage of the systematic review, a thorough search was carried out in various scientific databases, with the purpose of identifying relevant studies related to the application of Artificial Intelligence in the detection of cyber threats. Figure 2 presents an overview of the distribution of the recovered documents according to the provenance database. This representation facilitates the understanding of the proportion of studies provided by each source of information and allows to evaluate their coverage and thematic contribution with respect to the object of study, demonstrating the relative participation of each database in the conformation of the documentary corpus on Artificial Intelligence applied to the detection of cyber threats.

3.4 Exclusion Criteria

During the selection and purification phase of the recovered material, exclusion criteria were established to ensure that the studies included in the final analysis were relevant, current and methodologically sound. These criteria allowed to rule out documents that, despite having been identified through the defined search strategies, did not meet the scientific, thematic and methodological requirements established for this research. Consequently, the exclusion criteria (EC) applied in this systematic literature review were as follows:

Table 2. Search equations applied in the main scientific databases

Source	Search Equation
IEEE Xplore	(("Document Title":"artificial intelligence") OR ("Document Title":"ai") OR ("Document Title":"machine learning") OR ("Document Title":"deep learning") OR ("Document Title":"hybrid models")) AND (("Document Title":"cyber attack detection") OR ("Document Title":"cyber threat detection") OR ("Document Title":"ids") OR ("Document Title":"intrusion detection system") OR ("Document Title":"intrusion detection") OR ("Document Title":"real-time threat detection") OR ("Document Title":"security incident detection"))
Scopus	TITLE-ABS-KEY("artificial intelligence" OR "ai" OR "machine learning" OR "deep learning" OR "hybrid models") AND TITLE-ABS-KEY("cyber attack detection" OR "cyber threat detection" OR "intrusion detection system" OR "ids" OR "intrusion detection" OR "real-time threat detection" OR "security incident detection")
Web of Science	(TI=("artificial intelligence" OR "ai" OR "machine learning" OR "deep learning" OR "hybrid models") OR AK=("artificial intelligence" OR "ai" OR "machine learning" OR "deep learning" OR "hybrid models")) AND (TI=("cyber attack detection" OR "cyber threat detection" OR "intrusion detection system" OR "ids" OR "intrusion detection" OR "real-time threat detection" OR "security incident detection") OR AK=("cyber attack detection" OR "cyber threat detection" OR "intrusion detection system" OR "ids" OR "intrusion detection" OR "real-time threat detection" OR "security incident detection"))
Springer Link	("artificial intelligence" OR "ai" OR "machine learning" OR "deep learning" OR "hybrid models") AND ("cyber attack detection" OR "cyber threat detection" OR "ids" OR "real-time threat detection" OR "security incident detection")
ACM Digital Library	(([Title:"artificial intelligence"] OR [Title:ai] OR [Title:"machine learning"] OR [Title:"deep learning"] OR [Title:"hybrid models"] OR [Keywords:"artificial intelligence"] OR [Keywords:ai] OR [Keywords:"machine learning"] OR [Keywords:"deep learning"] OR [Keywords:"hybrid models"] OR [Abstract:"artificial intelligence"] OR [Abstract:ai] OR [Abstract:"machine learning"] OR [Abstract:"deep learning"] OR [Abstract:"hybrid models"]) AND ([Title:"cyber-attack detection"] OR [Title:"cyber threat detection"] OR [Title:ids] OR [Title:"intrusion detection system"] OR [Title:"intrusion detection"] OR [Title:"real-time threat detection"] OR [Keywords:"cyber-attack detection"] OR [Keywords:"cyber threat detection"] OR [Keywords:ids] OR [Keywords:"intrusion detection system"] OR [Keywords:"intrusion detection"] OR [Keywords:"real-time threat detection"] OR [Abstract:"cyber-attack detection"] OR [Abstract:"cyber threat detection"] OR [Abstract:ids] OR [Abstract:"intrusion detection system"] OR [Abstract:"intrusion detection"] OR [Abstract:"real-time threat detection"]))

- CE1: Documents are Books or Chapters of Book or Thesis or Papers of Systematic Review or Bibliometric Review.
- CE2: Items are older than 7 years.
- CE3: The papers are written in languages other than English.
- CE4: Not have full access to the items.
- CE5: The titles and keywords of the papers are not very suitable.
- CE6: The summary of the papers is not very relevant.
- CE7: It's a short paper.
- CE8: Papers are repeated.

3.5 Study Selection

The PRISMA diagram is a fundamental visual tool for clearly, structured and reproducible representing the process of document selection and screening in a systematic or bibliometric review. This approach allows to document each of the methodological stages: identification, screening, evaluation of eligibility and final inclusion, guaranteeing the transparency and traceability of the decisions taken during the documentary analysis. Through its application, it was possible to visualize in detail the path of the initially identified records until forming the final set of studies included in the review.

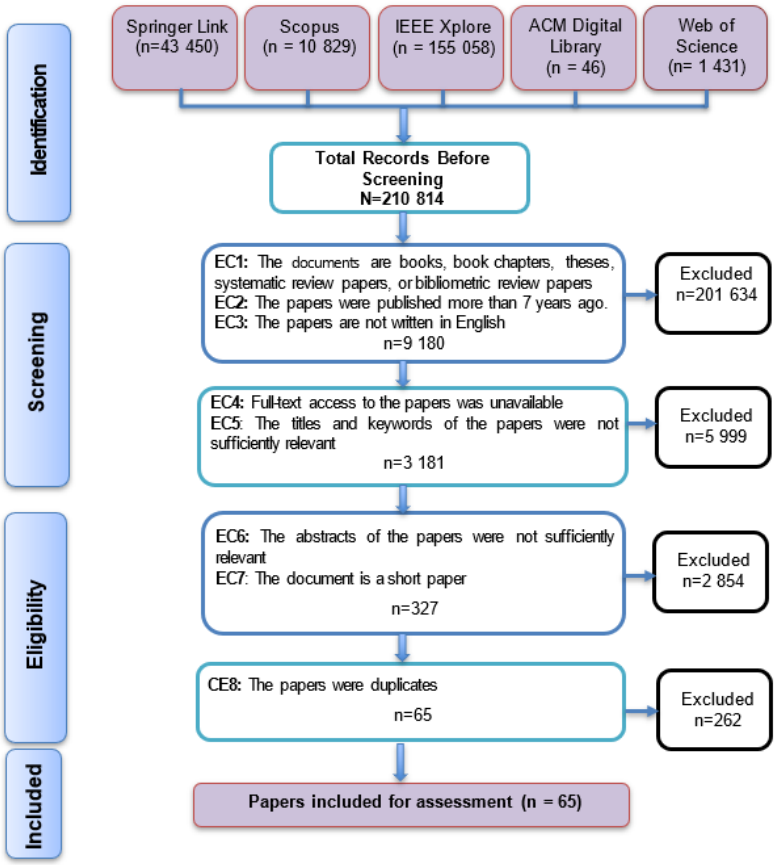

Fig. 3 PRISMA flow diagram

Figure 3 presents the corresponding PRISMA diagram, in which the applied filtering steps, the exclusion criteria used and the number of records resulting after each phase of the process are detailed.

3.6 Quality Assessment

In order to ensure the validity and reliability of the findings obtained in this systematic review, a rigorous process of evaluation of the methodological quality of the selected studies was developed. This phase allowed to identify possible sources of bias, assess the solidity of the collected evidence and verify that the included works met minimum standards of scientific rigor.

In order to facilitate their understanding, the Quality Assessment (QA1 to QA5) criteria were established, structured as sequential filters that allowed to assess the clarity of the research objectives, the suitability of the methodological approach, the validity of the instruments used, the coherence between the results and the conclusions, and the relevance and validity of the publications.

Only the studies that adequately satisfied these criteria were incorporated into the final synthesis of the review, thus ensuring the consistency and rigor of the evaluative process.

– QA1. Are the objectives of the research clearly specified?

Table 3. Application of quality criteria

Ref.	Paper	Type	QA1	QA2	QA3	QA4	QA5	Score
[1]	Ring et al. (2021)	Journal	3	3	3	3	2	14
[2]	Sun et al. (2024)	Conference	3	3	3	3	2	14
[3]	Rani et al. (2023)	Journal	3	3	3	2	2	14
[4]	Sana et al. (2024)	Journal	3	3	3	3	2	14
[5]	Khan et al. (2023)	Journal	2	3	3	3	3	14
[6]	Chinnasamy et al. (2025)	Journal	3	3	3	2	3	14
[7]	Gul et al. (2024)	Journal	3	2	3	3	3	14
[8]	Sale et al. (2024)	Journal	3	2	3	3	3	14
[9]	Behiry et al. (2024)	Journal	3	3	3	2	3	14
[10]	Yang et al. (2025)	Journal	3	3	2	3	3	14
[11]	Nasreen et al. (2024)	Journal	3	3	3	2	3	14
[12]	Muda et al. (2023)	Journal	3	3	3	2	3	14
[13]	Khan et al. (2025)	Journal	3	3	3	2	2	13
[14]	Sarhan et al. (2024)	Journal	3	3	3	2	2	13
[15]	Odeh & Taleb (2024)	Journal	3	3	3	3	2	13
[16]	Talukder et al. (2024)	Journal	2	3	3	3	2	13
[17]	Lai et al. (2024)	Journal	2	3	3	2	3	13
[18]	Lee et al. (2019)	Journal	2	3	3	3	2	13
[19]	Alsolami et al. (2024)	Journal	2	3	3	2	3	13
[20]	Mamatha et al. (2025)	Journal	3	3	3	2	2	13
[21]	Jullian et al. (2023)	Journal	3	3	3	2	2	13
[22]	Talukder et al. (2024)	Journal	3	3	3	2	2	13
[23]	Kushal et al. (2024)	Journal	3	2	2	3	3	13
[24]	Anthony et al. (2024)	Journal	3	2	2	3	3	13
[25]	Laghrissi et al. (2021)	Journal	3	2	3	3	2	13
[26]	Munir et al. (2019)	Journal	3	2	3	3	2	13
[27]	Ali et al. (2025)	Journal	3	2	2	3	3	13
[28]	Yaras & Dener (2024)	Journal	2	3	3	3	2	13
[29]	Wu et al. (2022)	Journal	2	3	2	3	3	13
[30]	Ullah & Mahmoud (2021)	Journal	2	2	3	3	2	13
[31]	Sajid et al. (2024)	Journal	3	2	2	3	3	13
[32]	Alsirhani et al. (2025)	Journal	3	2	3	2	3	13
[33]	Qazi et al. (2024)	Journal	3	2	2	3	3	13
[34]	Koca et al. (2021)	Journal	3	2	3	3	2	13
[35]	Hariharan et al. (2025)	Journal	3	2	3	3	2	13
[36]	Althobaiti & Escorcia (2024)	Journal	3	2	3	2	3	13
[37]	Kaushik et al. (2025)	Journal	3	2	3	3	2	13
[38]	Othman et al. (2023)	Journal	3	2	2	3	3	13

– QA2. Is the design of the study suitable for achieving these goals?

– QA3. Are the techniques used precisely described and their choice justified?

– QA4. Are data collection methods properly detailed?

– QA5. Are the collected data presented and properly described?

Table 4. Application of quality criteria

Ref.	Paper	Type	QA1	QA2	QA3	QA4	QA5	Score
[39]	Falowo et al. (2024)	Journal	3	2	2	3	3	13
[40]	Khayat et al. (2025)	Journal	3	2	3	3	2	13
[41]	Hussain et al. (2024)	Journal	3	2	3	2	3	13
[42]	Soltani et al. (2024)	Journal	3	2	3	3	2	13
[43]	Doas & Osama (2023)	Journal	3	2	3	3	2	13
[44]	Cavusoglu (2019)	Journal	3	2	3	3	2	13
[45]	Agarwal et al. (2021)	Journal	3	2	2	3	3	13
[46]	Yang & Lim (2021)	Journal	3	2	3	3	2	13
[47]	Abdullah (2024)	Journal	3	2	2	3	3	13
[48]	Elsaid et al. (2024)	Conference	3	2	2	2	3	12
[49]	Ahmed et al. (2024)	Conference	3	3	1	3	3	12
[50]	Zhao W. & Zhao Z. (2024)	Journal	3	2	3	2	2	12
[51]	Logeswari et al. (2023)	Journal	3	2	3	1	3	12
[52]	Alghamdi & Bellaiche (2023)	Journal	3	2	3	3	1	12
[53]	Pavithra & Venkata (2024)	Journal	3	2	2	3	2	12
[54]	Bella et al. (2024)	Journal	3	2	2	2	3	12
[55]	Keshik et al. (2023)	Journal	3	2	3	2	2	12
[56]	Vinayakumar et al. (2019)	Journal	3	2	3	3	1	11
[57]	Liu et al. (2021)	Journal	2	2	3	3	1	11
[58]	Megantara & Ahmad (2021)	Journal	2	2	3	1	3	11
[59]	Aljuaid & Alshamrani (2024)	Journal	2	2	1	3	3	11
[60]	Samy et al. (2020)	Journal	2	2	3	3	1	11
[61]	Hnamte et al. (2023)	Journal	2	2	3	3	1	11
[62]	Bassam et al. (2023)	Journal	1	1	3	2	1	9
[63]	Ziqui et al. (2024)	Journal	1	1	1	3	2	9
[64]	Lisong et al. (2024)	Journal	2	2	2	0	2	8
[65]	Muhammad et al. (2023)	Journal	1	0	3	2	2	8

The quality criteria comprise 5 questions intended to rigorously evaluate the filtered papers. This procedure is the last methodological filter before conducting the thorough review of the selected studies and answering the research questions raised.

From the above, the quality criteria were applied to the 65 identified papers, through a structured evaluation procedure that allows homogeneously assessing the methodological robustness and scientific relevance of each included study.

To facilitate the interpretation of the results, Table 3 presents the application of the evaluation criteria.

Each question was rated by an ordinal scale, where 0 corresponds to “does not fulfill”, 1 to “low”, 2 to “regular” and 3 to “good”.

Papers with a score greater than 10 were considered eligible to integrate the systematic review, while those with a score of less than or equal to 10 were excluded from the final analysis.

The 65 papers were verified according to these criteria, obtaining 61 selected studies; the four excluded papers belonged to the ACM Digital Library of the final corpus.

3.7 Data Extraction Strategies

The data extraction strategy is a fundamental stage in a systematicreview, as it requires intuitive and accessible tools that facilitate the organization and storage of the selected studies. The management of the scientific papers was carried out using Mendeley Desktop v1.19.8, where they were organized alphabetically by author; later, Figure 4 presents a screenshot of the documentary set previously selected for this systematic review in the study. This protocol has been applied analogously in recent systematic reviews of Artificial Intelligence in other domains, such as the diagnosis of neoplastic diseases [92], which supports its validity as a methodological framework for systematizing evidence in this field.

3.8 Synthesis of Findings

A comprehensive review of the selected papers was carried out with the purpose of collecting and systematizing relevant information from each study using Mendeley Desktop, obtaining fundamental inputs for the academic synthesis that will be presented in the results and discussion sections.

Likewise, Mendeley was used as a bibliographic manager to organize, consult and control the papers analyzed; complementary, RAj (Research Assistant) was used, developed by Javier Gamboa-Cruzado, as a support tool for the analysis of relevant information.

4 Results and Discussion

This section presents and analyzes the results obtained in relation to the theoretical framework on the application of artificial intelligence in the detection of cyberattacks and with the objectives defined in the research.

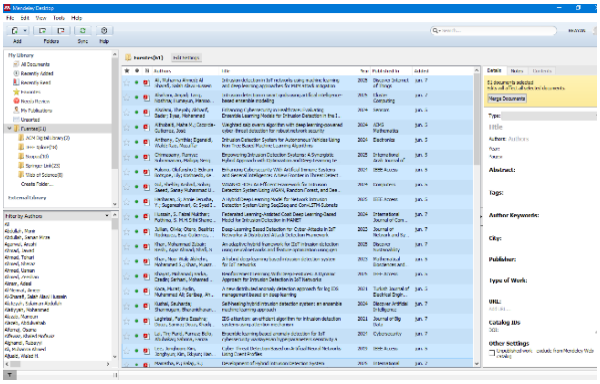

Fig. 4. Data management on the Mendeley desktop platform

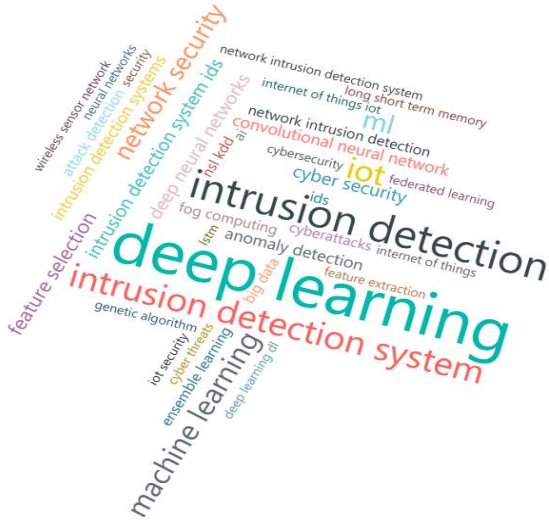

Fig. 5. Keyword cloud

The analysis of the selected studies was developed through a combined strategy that integrated a comprehensive review with automated data processing techniques based on artificial intelligence, which allowed to strengthen the interpretation of the findings.

4.1 Overview of Studies

To facilitate the general understanding of the studied area, the relationships present in the bibliometric network were analyzed in detail, complementing the analysis by two graphs that represent the frequency of keywords.

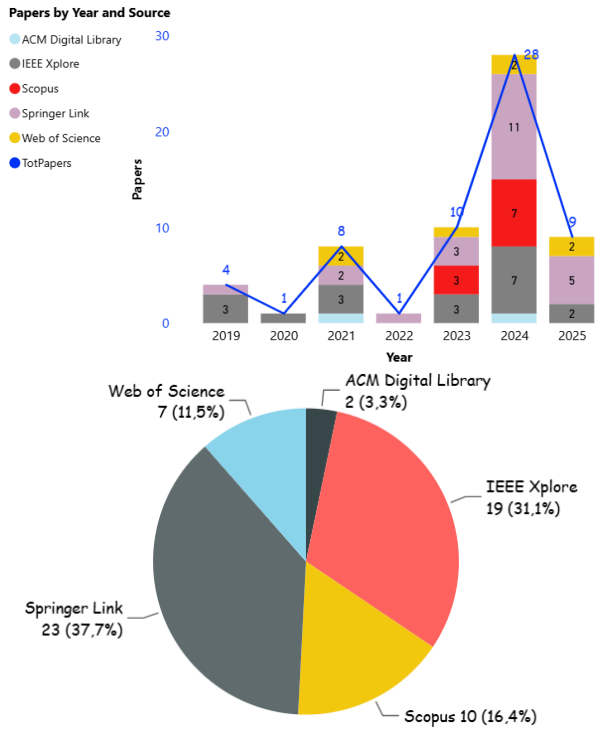

Fig. 6. Number of papers per year and source

Figure 5 presents a keyword cloud that visually synthesizes the predominant terms in selected studies on Artificial Intelligence and cyberattack detection.

Its incorporation allows to recognize the thematic structure of the analyzed corpus and to identify the technologies, approaches and domains that concentrate greater attention within the examined literature.

According to the observed distribution, the prominence of “deep learning”, “intrusion detection” and “intrusion detection system” evidences that the literature focuses its attention on advanced models aimed at identifying malicious behaviors.

The joint presence of “machine learning”, “convolutional neural network”, “LSTM” and “feature selection” suggests that this trend responds to the need to extract complex patterns and improve discriminative capacity. Likewise, terms like “cybersecurity”, “network security” and “internet of things” reflect technological scenarios where these capabilities acquire increasing operational relevance.

In comparison, Guembe and collaborators [66] identified cybersecurity, deep learning, learning systems and learning algorithms as predominant keywords; instead, Ofusori and his team [68] highlighted machine learning, artificial cybersecurity intelligence, and deep learning, demonstrating a greater concentration in approaches directly associated with artificial intelligence applied to cybersecurity. It should be noted that Albahri and Al Amoodi [69] mainly pointed out artificial intelligence, deep learning and machine learning; therefore, a thematic convergence between the studies is observed, although with differences in the breadth of the terms used. Overall, the results show that artificial intelligence, machine learning, deep learning and cybersecurity are the most recurrent conceptual axes, which reinforces their centrality within the analyzed literature.

These findings support the transfer of approaches based on deep learning and intrusion detection to business sectors with digital infrastructures, IoT networks and cybersecurity-intensive needs, provided that the models are validated in accordance with the operational context. Likewise, its application in other regions and periods requires comparing bibliometric patterns, updating technological vocabularies and evaluating the evolution of emerging techniques.

Figure 6 presents the temporal distribution of the 61 studies selected between 2019 and 2025, as well as their origin according to the five academic sources considered. This representation allows to simultaneously examine the evolution of scientific production and the relative weight of each source in the conformation of the analyzed corpus.

From the reported results, scientific production shows an irregular trajectory, with a marked growth since 2023 and a maximum of 28 publications in 2024, which shows a recent concentration of research interest.

The reduction to nine works in 2025 indicates a lower documentary presence than the previous maximum, without altering the observed temporal concentration. By sources, Springer Link and IEEE Xplore gather 68.8% of the selected corpus, suggesting that both platforms mainly structure the analyzed documentary coverage.

In comparison, Lansky and co-authors [70] identified IEEE as the most represented source,

Table 5. Programming languages used in Artificial Intelligence

Programming Language	Reference	Qty.
Scala	[2] [4] [9] [14] [17] [20] [22] [27] [29] [33] [34] [35] [36] [41] [44] [45] [46] [47] [50] [54] [57] [60] [61]	23 (39)
Python	[1] [3] [4] [7] [8] [10] [11] [14] [15] [16] [17] [20] [22] [24] [26] [27] [31] [34] [38] [39] [40] [41] [45] [46] [48] [49] [51] [52] [53] [54] [56] [58] [59]	33 (56)
Java	[4] [37]	2 (3)
C++	[51]	1 (2)

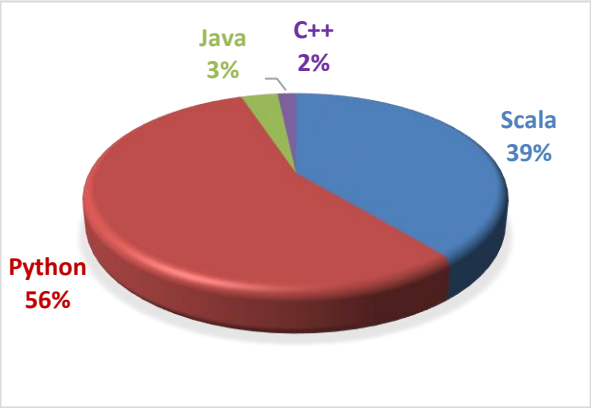

Fig. 7. Distribution of programming languages

with 59%, followed by Elsevier with 21%; instead, Valdivia and colleagues [71] reported a more diversified distribution, in which Wiley Online Library reached 22.4% and ACM Digital Library 15.2%, along with the presence of other sources such as Web of Science, Scopus and ScienceDirect. Although both studies show a concentration of publications on certain platforms, it should be noted that the magnitude of this concentration differs between them; therefore, the results suggest variations in the documentary coverage and the origin of the studies analyzed.

Taken together, these differences show that distribution by source may depend on the search strategy and the bases considered in each review.

These results allow to guide future revisions towards business sectors intensive in digital infrastructure, especially considering the sources that concentrate greater production, although without excluding bases with less representation to avoid coverage biases.

In other regions and periods, it is advisable to replicate the temporal and source analysis, incorporating comparable longitudinal windows that allow to evaluate stability, expansion or redistribution of scientific knowledge.

4.2 Answers to the Research Problems

This section presents the answers to the research questions asked, based on the systematic analysis of the selected studies. The synthesis of the evidence allows to integrate findings from different methodological approaches, identifying relevant patterns, convergences and discrepancies. In this way, a structured interpretation of the results is provided that contributes to rigorously respond to the objectives set out in the study.

4.2.1 RQ1: Which Programming Languages are Used for the Development of AI-Based Solutions?

Table 4 and Figure 7 present the distribution of the programming languages identified in studies developing solutions based on Artificial Intelligence, considering their frequency and percentage participation.
This information is relevant because it allows to recognize the predominant implementation technologies and establish the degree of concentration of the tools used within the scientific corpus analyzed.

As seen in the findings, Python concentrates 56% of the identified occurrences, positioning itself as the predominant language versus Scala, which represents 39%.

Taken together, both languages gather 95% of the records, demonstrating a marked technological concentration and suggesting that the AI solutions examined preferentially resort to a reduced set of programming environments. In contrast, Java and C++ reach only 3% and 2%, respectively, reflecting a comparatively marginal presence within the selected studies.

Table 6. Criteria of cyberattack detection

Criterion	Reference	Qty. (%)
Detection Rate	[1] [2] [3] [5] [7] [10] [12] [13] [14] [15] [17] [18] [19] [20] [21] [24] [28] [29] [31] [32] [33] [34] [36] [38] [39] [46] [47] [48] [50] [51] [53] [54] [55] [56] [57] [59] [60] [61]	38 (52)
False Positive Rate	[1] [3] [5] [9] [13] [15] [16] [18] [19] [21] [24] [26] [28] [30] [31] [33] [38] [45] [46] [54] [56] [61]	22 (30)
Detection Time	[21] [23] [34] [53] [55] [61]	6 (8)
Response Time	[10] [25] [36] [47] [48] [49] [61]	7 (10)

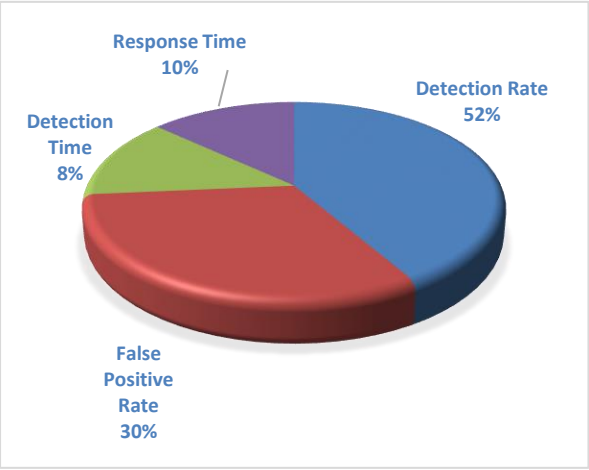

Fig. 8. Detection rate and response

In comparison, Lansky and his team [70] reported that Python was present in 22% of the studies analyzed, while Java reached 4%; instead, Edje and collaborators [72] identified the use of Python in 13 papers and Java in 3, which again evidences a greater presence of Python.

For their part, Özgür and Erdem [73] found a different distribution, with Java used in 8 papers and C++ in 5, while Arqane and co-authors [74] noted that Python was present in 44% of the studies examined.

The high concentration in Python and Scala suggests that future AI applications in business, industrial or institutional sectors could prioritize these languages when it is sought to maintain coherence with the technological trends identified, although their selection must respond to the specific characteristics of each environment.

Methodologically, replicating this analysis in other regions and periods would allow to determine whether this concentration remains stable or changes as the tools used to develop intelligent solutions evolve.

4.2.2 RQ2: What Citeria are Used to Evaluate the Performance of Cyberattack Detection?

Table 5 and Figure 8 present the main criteria used to evaluate the performance of Cyberattack Detection, considering their frequency of onset and percentage participation in the studies analyzed. This distribution allows to identify which dimensions of performance receive the most attention in the literature and to assess the balance between detection efficiency, generation of false alarms and temporal response capacity.

According to the identified pattern, Detection Rate concentrates 52% of occurrences and is the predominant criterion, indicating that the ability to correctly identify attacks represents the main assessment dimension in the studies examined. False Positive Rate reaches 30%, showing that the reduction of false alarms is an essential complement to performance, since a high detection capacity loses practical utility when it generates incorrect classifications.

In contrast, Response Time and Detection Time represent 10% and 8%, respectively, suggesting that the literature analyzed prioritizes discriminatory efficacy over the temporal dimensions of the detection and response process.

In comparison, Lansky and colleagues [70] incorporated Detection Rate as one of the parameters used to evaluate the revised papers, while Chinnasamy and collaborators [75] identified four studies that employed this criterion.

It should be noted that Satilmiş and his team [90] reported a broader presence of performance metrics, with 18 papers using Detection Rate and 11 that they considered False Positive Rate.

Instead, Khalaf and co-authors [77] analyzed 10 segmented papers between statistical and AI approaches, providing a complementary perspective on the evaluation of the systems examined.

Bar and colleagues [78] identified four papers that used Detection Time as an evaluation criterion.

This convergence extends to adjacent detection domains: Cardenas-Quispe et al. [76], in a systematic review on machine learning for malware detection in Android, identified the high rate of true positives (38.52%) and the low rate of false positives (37.04%) as the predominant effectiveness criteria, which reinforces - from a different subdomain - the centrality of the detection capacity and control of false positives as the most

These results suggest that the evaluation of Cyberattack Detection solutions in business, industrial, financial or institutional sectors should simultaneously integrate detection capacity, false positive control and temporary metrics, avoiding evaluating performance through a single indicator.

Also, replicating this analysis in other regions and periods would allow to determine whether the relevance of the temporal criteria increases as operational environments and response requirements against cyber threats evolve.

4.2.3 RQ3: What are the Quartile Levels of Journals that Publish Research on the Effect of Artificial Intelligence on Cyberattack Detection?

Table 6 and Figure 9 present the distribution of the 61 papers according to the journals' quartile, supplemented by citation indicators and the relationship of these levels to the sources and years of publication. This characterization is relevant because it allows to evaluate the quality and impact of the scientific corpus used to analyze Artificial Intelligence applied to the Detection of Cyberattacks.

Based on the evidence presented, papers published in Q1 journals predominate clearly, with 39 studies equivalent to 63.9% of the corpus, followed by Q2 with 18 papers (29.5%), while Q3 and unranked publications account for only 3.3% each. This concentration in Q1 and Q2, which together reaches 93.4%, shows that the review is mostly supported in literature published in journals of high relative position within its categories. In addition, the Q1 papers accumulate 1,886 of the 2,337 registered citations and present 48 citations per paper, compared to 24 in Q2, which reinforces its greatest academic influence within the analyzed set.

Table 7. Impact of papers per quartile

Quartile	No. of Papers	No. of Citations	Citations per Paper	H Index
Q1	39	1886	48	7363
Q2	18	433	24	1220
Q3	2	3	2	52
NQ	2	15	8	41
Total	**61**	**2337**	**38**	**8676**

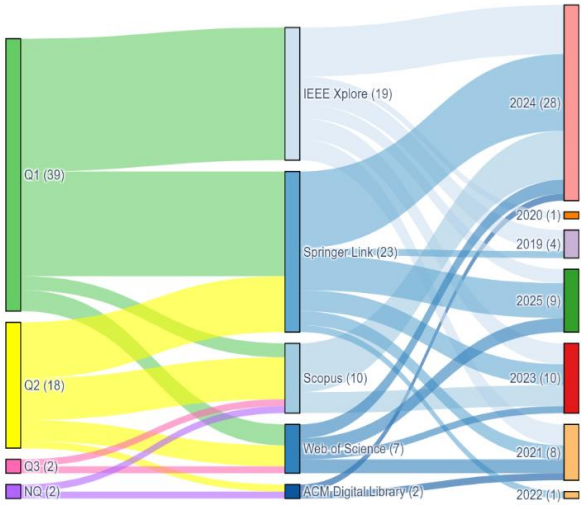

Fig. 9. Quartile-source relational diagram

In comparison, Padilla-Gómez and her team [79] reported, within a set of 70 publications, 47 papers in Q1, 20 in Q2 and 2 in Q3 journals, showing a marked concentration in the higher quartiles. Raimundo and Rosário [80] identified 7 Q1 journals, 6 Q2 and 5 Q3, showing a more balanced distribution between the three levels. Instead, Padilla and co-authors [81] recorded 3 Q2 journals with 6 publications and 4 Q3 journals with 10 publications, reflecting a greater documentary representation in Q3.

Finally, Raymundo and Rosario [82] reported 11 Q1 journals, 3 Q2 and 2 Q3; it should be noted that this distribution again presents a predominance of sources located in the upper quartile.

Table 8. Classification of definitions synthesized by category

Synthesized Definition	Category	Reference	Qty. (%)
Use artificial intelligence algorithms to automate tasks such as pattern classification and detection, improving efficiency and accuracy in processes that traditionally require human intervention.	Functional	[1] [2] [5] [7] [10] [13] [15] [17] [18] [19] [20] [24] [25] [28] [29] [31] [33] [35] [36] [37] [40] [41] [44]	23 (38,3)
Development of advanced machine learning and deep learning models, such as neural networks, to analyze large volumes of data, identify patterns and make autonomous decisions based on these analyses.	Technical	[3] [4] [6] [8] [9] [11] [12] [14] [16] [22] [23] [26] [27] [30] [32] [34] [38] [39] [42] [43] [45] [46] [47] [48]	24 (40,0)
Implementation of predictive models and AI algorithms in practical areas such as cybersecurity and automotive, optimizing intrusion detection and improving real-time decision-making.	Applied	[49] [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61]	13 (21,7)

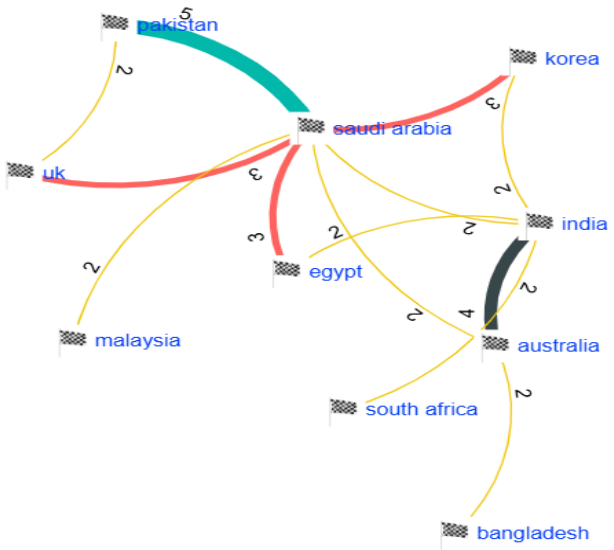

Fig. 10. Countries with greater frequency of co-occurrence

The high representation of Q1 and Q2 publications provides a solid scientific basis for transferring the findings to business, industrial and institutional contexts.

Here the Detection of Cyberattacks constitutes a strategic need, although their applicability must be validated according to the specific conditions of each sector.

In addition, future research could replicate this distribution by quartiles in other regions and periods to determine whether concentration in high-impact journals is maintained and evaluate possible temporal or geographical variations in field maturity.

4.2.4 RQ4: What Conceptual Definitions have been Proposed in the Studies on Artificial Intelligence Applied to Cyberattack Detection?

Table 7 summarizes the conceptual definitions identified in the studies on Artificial Intelligence applied to Cyberattack Detection, grouping them into three categories: functional, technical and applied.

This classification is relevant because it allows to recognize how the literature conceptualizes Artificial Intelligence from its operational

Table 9. Informative table of co-occurrence stocks

Country1	Country2	Weight
pakistan	saudi arabia	5
australia	india	4
egypt	saudi arabia	3
korea	saudi arabia	3
saudi arabia	uk	3
australia	bangladesh	2
australia	saudi arabia	2
egypt	india	2
india	korea	2
india	saudi arabia	2
india	south africa	2
malaysia	saudi arabia	2
pakistan	uk	2
Total		**34**

Table 10. Top citations and their network metrics in the coocurrences network

Country	Degree	Strength	Clustering Coefficient	Betweenness
saudi arabia	0,78	20,00	0,10	0,72
india	0,56	12,00	0,14	0,25
australia	0,33	8,00	0,17	0,22
pakistan	0,22	7,00	0,62	0,00
egypt	0,22	5,00	0,46	0,00
korea	0,22	5,00	0,46	0,00
uk	0,22	5,00	0,62	0,11
bangladesh	0,11	2,00	0,00	0,00
malaysia	0,11	2,00	0,00	0,00
south africa	0,11	2,00	0,00	0,00
Total	**2,89**	**68,00**	**2,57**	**1,31**

capabilities, its technological fundamentals and its specific areas of application.

According to the observed distribution, the technical category concentrates 40% of the studies, followed by the functional with 38.3% and the applied with 21.7%, demonstrating a predominance of conceptualizations oriented to machine learning models, deep learning and neural networks.

The proximity between the technical and functional categories suggests that literature closely links algorithmic architecture with its ability to automate tasks, recognize patterns, and improve process accuracy. The lower representation of the applied category indicates that the definitions focus mainly on the mechanisms and capabilities of Artificial Intelligence, while their contextualization in specific cybersecurity and real-time decision-making scenarios presents a relatively lower presence.

In comparison, Valdivieso and collaborators [83] conceptualize Artificial Intelligence applied to Cyberattack Detection as a set of techniques aimed at processing large volumes of data and threat identification; instead, Li and Liu [84] expand this perspective by incorporating threat classification and risk prediction capabilities through data analysis. For their part, Zhang and his team [85] introduce a complementary dimension through explanable Artificial Intelligence (XAI), emphasizing the transparency and understanding of the models as relevant elements to strengthen trust in cybersecurity systems.

This conceptual structure can guide the transfer of AI solutions to business, industrial and technological sectors, clearly differentiating between technical foundations, expected functionalities and application scenarios before implementing Cyberattack Detection systems. Also, replicating this classification in other regions and periods would allow to examine whether the definitions evolve from predominantly technical approaches to more applied perspectives, providing a methodological basis for comparing the conceptual maturity of the field.

4.2.5 RQ5: Which Countries have the Highest Frequency of Co-Occurrence in Research on Artificial Intelligence Applied to Cyberattack Detection?

Figure 10, Table 8 and Table 9 characterize the international co-occurrence structure of the studies on Artificial Intelligence applied to Cyberattack Detection, showing both the intensity of the relationships between countries and their main network metrics. This analysis is relevant because

it allows countries with the greatest relational presence to be identified, recognizes the most intense international links and determines which nodes play central positions within the bibliometric structure examined.

As seen in the findings, Saudi Arabia presents the greatest strength of connection, with a value of 20, followed by India with 12 and Australia with 8, which evidences a structure of concentrated co-occurrence around a small number of countries.

This centrality of Saudi Arabia is structurally explained by its repeated participation in links with Pakistan, Egypt, Korea, the United Kingdom, Australia, India and Malaysia, especially with the Pakistan-Saudi Arabic relationship with weight 5, the greatest intensity recorded. In addition, its high intermediation of 0.72, compared to 0.25 in India and 0.22 in Australia, indicates that Saudi Arabia occupies an articulating position within the network, while countries such as Pakistan and the United Kingdom have clustering coefficients of 0.62, reflecting greater relative cohesion between their immediate connections.

In comparison, Guembe and colleagues [66] stand out for India for its participation in international collaborations and for the impact of its research, even though it has a smaller volume of publications than other countries.

For their part, Koca and collaborators [86] place China among the countries with the highest scientific production, although with a lower frequency of citation than that observed in the United States.

Instead, Yilmaz [87] identifies the United States as one of the main references in terms of production and scientific impact.

It should be noted that Judijanto and his team [88] also point to the relevance of Saudi Arabia and Australia, whose comparatively minor production is accompanied by a high citation, while Goranin [89] highlights the participation of Canada and various European countries for the impact of their research.

The concentration of relations in Saudi Arabia, India and Australia suggests that future research and business projects on Artificial Intelligence and Cyberattack Detection could consider these nodes as benchmarks for expanding cooperation networks towards technology, financial, industrial and digital services sectors.

Also, replicating this analysis in other regions and periods would allow to evaluate the stability of these positions, identify new hubs of collaboration and determine if the international structure of the field evolves towards more diversified networks or remains concentrated in certain countries.

4.2.6 RQ6: What thematic categories predominate in the scientific production on Artificial Intelligence applied to Cyberattack Detection?

Figure 11 and Table 10 present the thematic structure derived from the co-occurrence of keywords, where centrality expresses the degree of relevance of each topic within the field and density represents its level of internal development. This representation allows to distinguish specialized and marginal issues, as well as simultaneously evaluate their degree of consolidation and their articulation with the general structure of the research on Artificial Intelligence applied to the Detection of Cyberattacks.

From the reported results, IoT Security and Intrusion Detection are positioned as specialized topics due to their high densities of 0.84 and 0.55, respectively, although their centralities of 0.35 and 0.34 reveal a relatively limited integration with the thematic set. In contrast, seven of the nine topics identified belong to the marginal category, showing moderate centralities but reduced densities, which evidences lines related to machine learning, deep learning and neural networks still insufficiently developed internally. Particularly, Deep Learning Security records 4,472 citations and 101 documents, but maintains a density of 0.22 and a centrality of 0.41, demonstrating that high production and scientific impact do not necessarily imply greater maturity or structural centrality of the subject.

In comparison, Ofusori and his team [68] highlight the need to continue innovating in the Artificial Intelligence techniques applied to cybersecurity, which evidences the constant evolution of the thematic lines associated with this field. For their part, Padilla and co-authors [81] structure scientific production in four thematic fields, among which the one related to maritime cybersecurity acquires special relevance. While both studies address different thematic contexts and structures, it should be noted that they agree

that they agree to evidence the progressive diversification of cybersecurity research and the need to strengthen specialized approaches.

Specialized topics can be benchmarks for developing focused Cyberattack Detection solutions in industrial, financial, technological, or IoT-intensive organizations, while marginal issues represent opportunities to strengthen research, methodological integration, and development of emerging applications. Also, replicating the thematic map in other regions and periods would allow to determine if the keywords associated with machine learning and deep learning evolve towards positions of greater density and centrality, providing evidence on the transformation and temporal maturation of the scientific domain.

5 Conclusions and Future Research

The systematic review and bibliometric analysis allow us to conclude that the application of Artificial Intelligence in the Detection of Cyberattacks constitutes an expanding field characterized by a growing technological specialization, but also by asymmetries in the way in which their solutions are developed, evaluated, conceptualized and articulated. Rather than evidence of a homogeneous evolution, the results reveal a scientific domain in the process of consolidation, where certain approaches concentrate attention while other dimensions necessary for their maturity remain less developed.

At the technical-evaluative level, the integration of RQ1 and RQ2 shows a marked concentration in both the programming environments used and the criteria used to assess performance. This convergence favors some technological and methodological standardization; however, it also shows a dependence on a small set of tools and an evaluation oriented mainly towards the discriminative capacity of the systems. In this sense, the lower presence of temporal dimensions reveals a relevant evaluative asymmetry: the field has advanced more in determining whether attacks can be correctly identified than in establishing with equal depth the speed and opportunity with which such detection can occur in operational scenarios.

On the conceptual level, the RQ4 evidences that Artificial Intelligence applied to Cyberattack Detection continues to be predominantly defined from its technical mechanisms and functional capabilities. Although this orientation reflects a consolidated algorithmic basis, the lower presence of conceptualizations linked to specific application scenarios shows a gap between the development of technological capabilities and their operational contextualization. From this emerges a relevant theoretical question: the maturity of the field depends not only on perfecting models capable of classifying or predicting threats, but also on moving towards conceptual frameworks that integrate explanability, context of use and decision-making in real conditions.

From a bibliometric and thematic perspective, the RQ5 and RQ6 show that the scientific structure of the domain also does not present a uniform development. International collaboration is organized around certain nodes with articulating capacity, while the thematic configuration combines specialized areas with a broader set of still underconsolidated lines. This coexistence shows that high visibility or scientific production alone is not an indicator of thematic maturity. On the contrary, the development of the field also depends on the articulation between lines of research, the density of its internal relationships and the ability to transform emerging areas into coherent and connected scientific nuclei.

Taken together, the scientific knowledge that emerges from this review shows that the evolution of Artificial Intelligence applied to the Detection of Cyberattacks must be understood as a multidimensional process in which technology, evaluation, conceptualization, collaboration and thematic specialization converge. The main contribution of the study lies precisely in integrating these dimensions within the same analytical structure, surpassing a reading focused exclusively on algorithms or architectures. In this way, it is evident that the current challenge of the field is not only to develop more advanced models, but to achieve a balance between technical performance, more complete evaluation criteria, conceptual maturity, diversification of scientific cooperation and consolidation of the emerging thematic lines.

Future research should broaden the analysis towards other regional periods and contexts, deepen temporal and operational evaluation

criteria, examine the evolution from predominantly technical conceptualizations to more applied approaches and analyze longitudinally the transformation of collaborative networks and the thematic categories, with the purpose of determining whether the current emerging lines reach higher levels of articulation and scientific maturity.

References

1. **Ring, J.H., Van Oort, C.M., Durst, S. (2021).** Methods for Host-Based Intrusion Detection with Deep Learning. Digital Threats: Research and Practice, Vol. 2, No. 4, pp. 1–29. DOI: 10.1145/ 3461462.
2. **Sun, Z., Teixeira, A., Toor, S. (2024).** GNN-IDS: Graph Neural Network Based Intrusion Detection System. Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024), pp. 1–12. DOI: 10.1145/3664476. 3664515.
3. **Rani, S.V.J., Ioannou, I., Nagaradjane, P. (2023).** A Novel Deep Hierarchical Machine Learning Approach for Identification of Known and Unknown Multiple Security Attacks in a D2D Communications Network. IEEE Access, Vol. 11, pp. 95161–95179. DOI: 10.1109/access.2023.3308036.
4. **Sana, L., Nazir, M., Yang, J. (2024).** Securing the IoT Cyber Environment: Enhancing Intrusion Anomaly Detection with Vision Transformers. IEEE Access, Vol. 12, pp. 82443–82459. DOI: 10.1109/access.2024.3 404778.
5. **Khan, N.W., Alshehri, M.S., Khan, M.A. (2023).** A Hybrid Deep Learning-Based Intrusion Detection System for IoT Networks. Mathematical Biosciences and Engineering, Vol. 20, No. 8, pp. 13491–13520. DOI: 10.3934/mbe.2023602.
6. **Chinnasamy, R., Subramanian, M., Sengupta, N. (2025).** Empowering Intrusion Detection Systems: A Synergistic Hybrid Approach with Optimization and Deep Learning Techniques for Network Security. The International Arab Journal of Information Technology, Vol. 22, No. 1, pp. 60–71. DOI: 10.34028/iajit/22/1/6.
7. **Gul, S., Arshad, S., Saeed, S.M.U. (2025).** WGAN-DL-IDS: An Efficient Framework for Intrusion Detection System Using WGAN, Random Forest, and Deep Learning Approaches. Computers, Vol. 14, No. 1. DOI: 10.3390/computers14010004.
8. **Saleh, H.M., Marouane, H., Fakhfakh, A. (2024).** Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning. IEEE Access, Vol. 12, pp. 3825–3842. DOI: 10.1109/access.2023. 3349248.
9. **Behiry, M.H., Aly, M. (2024).** Cyberattack Detection in Wireless Sensor Networks Using a Hybrid Feature Reduction Technique with AI and Machine Learning Methods. Journal of Big Data, Vol. 11, No. 16, pp. 1–39. DOI: 10.1186/s40537-023-00870-w.
10. **Yang, H., Effatparvar, M. (2025).** A Deep Learning-Based Intrusion Detection System for CAN Vehicle Based on Combination of Triple Attention Mechanism and GGO Algorithm. Scientific Reports, Vol. 15, DOI: 10.1038/s41598-025-04720-y.
11. **Fathima, A.H., Ibrahim, S.P.S., Khraisat, A. (2024).** Enhancing Network Traffic Anomaly Detection: Leveraging Temporal Correlation Index in a Hybrid Framework. IEEE Access, Vol. 12, pp. 136805–136825. DOI: 10.1109/access.2024.34589 03.
12. **Muda, S.R.B.T., Yusof, M.H.M., Alfawaz, K.M. (2023).** New Optimized Adaptive Time Series IDS Classifier Algorithm: Beyond Deep Learning. IEEE Access, Vol. 11, pp. 129882–129895. DOI: 10.1109/ access.2023.3334160.
13. **Khan, M.Z., Reshi, A.A., Shafi, S. (2025).** An Adaptive Hybrid Framework for IIoT Intrusion Detection Using Neural Networks and Feature Optimization Using Genetic Algorithms. Discover Sustainability, Vol. 6. DOI: 10.1007/s43621-025-01141-9.
14. **Sarhan, M., Layeghy, S., Moustafa, N. (2024).** Feature Extraction for Machine Learning-Based Intrusion Detection in IoT Networks. arXiv Preprint, arXiv:2108.12722v3. DOI: 10.1016/j.dcan.2022.08. 012.

15. **Odeh, A., Taleb, A.A. (2024).** Robust Network Security: A Deep Learning Approach to Intrusion Detection in IoT. CMC, Vol. 81, No. 3, pp. 4150–4167. DOI: 10.32604/cmc.2024. 058052.
16. **Talukder, M.A., Islam, M.M., Uddin, M.A. (2024).** Machine Learning-Based Network Intrusion Detection for Big and Imbalanced Data Using Oversampling, Stacking Feature Embedding and Feature Extraction. Journal of Big Data, Vol. 11. DOI: 10.1186/s40537-024-00886-w.
17. **Lai, T., Farid, F., Bello, A. (2024).** Ensemble Learning-Based Anomaly Detection for IoT Cybersecurity via Bayesian Hyperparameters Sensitivity Analysis. Cybersecurity, Vol. 7. DOI: 10.1186/s42400-024-00238-4.
18. **Lee, J., Kim, J., Kim, I. (2019).** Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles. IEEE Access, Vol. 7, pp. 165607–165617. DOI: 10.1109/access.2019. 2953095.
19. **Alsolami, T., Alsharif, B., Ilyas, M. (2024).** Enhancing Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection. Sensors, Vol. 24, No. 18. DOI: 10.3390/s24185937.
20. **Mamatha, P., Balaji, S., Anuraghav, S.S. (2025).** Development of Hybrid Intrusion Detection System Leveraging Ensemble Stacked Feature Selectors and Learning Classifiers to Mitigate the DoS Attacks. International Journal of Computational Intelligence Systems, Vol. 18. DOI: 10.1007/s44196-025-00750-6.
21. **Jullian, O., Otero, B., Rodríguez, E. (2023).** Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework. Journal of Network and Systems Management, Vol. 31. DOI: 10.1007/s10922-023-09722-7.
22. **Talukder, M.A., Sharmin, S., Uddin, M.A. (2024).** MLSTL-WSN: Machine Learning-Based Intrusion Detection Using SMOTETomek in WSNs. International Journal of Information Security, Vol. 23, pp. 2139–2158. DOI: 10.1007/s10207-024-00833-z.
23. **Kushal, S., Shanmugam, B., Sundaram, J. (2024).** Self-Healing Hybrid Intrusion Detection System: An Ensemble Machine Learning Approach. Discover Artificial Intelligence, Vol. 4. DOI: 10.1007/ s44163-024-00120-9.
24. **Anthony, C., Elgenaidi, W., Rao, M. (2024).** Intrusion Detection System for Autonomous Vehicles Using Non-Tree Based Machine Learning Algorithms. Electronics, Vol. 13, No. 5. DOI: 10.3390/electronics13050809.
25. **Laghrissi, F., Douzi, S., Douzi, K. (2021).** IDS-Attention: An Efficient Algorithm for Intrusion Detection Systems Using Attention Mechanism. Journal of Big Data, Vol. 8. DOI: 10.1186/s40537-021-00544-5.
26. **Munir, M., Siddiqui, S.A., Dengel, A. (2019).** DeepAnT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series. IEEE Access, Vol. 7, pp. 1991–2005. DOI: 10.1109/access.2018.2886457.
27. **Ali, M.A., Al-Sharafi, S.A.H. (2025).** Intrusion Detection in IoT Networks Using Machine Learning and Deep Learning Approaches for MitM Attack Mitigation. Discover Internet of Things, Vol. 5, No.. 48. DOI: 10.1007/s43926-025-00104-w.
28. **Yaras, S., Dener, M. (2024).** IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm. Electronics, Vol. 13, No. 6. DOI: 10.3390/ electronics13061053.
29. **Wu, T., Fan, H., Zhu, H. (2022).** Intrusion Detection System Combined Enhanced Random Forest with SMOTE Algorithm. EURASIP Journal on Advances in Signal Processing, Vol. 39, pp. 1–20. DOI: 10.1186/s13634-022-00871-6.
30. **Ullah, I., Mahmoud, Q.H. (2021).** Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks. IEEE Access, Vol. 9, pp. 103906–103923. DOI: 10.1109/access. 2021.3094024.
31. **Sajid, M., Malik, K.R., Almogren, A. (2024).** Enhancing Intrusion Detection: A Hybrid Machine and Deep Learning Approach. Journal of Cloud Computing, Vol. 13. DOI: 10.1186/s13677-024-00685-x.
32. **Alsirhani, A., Tariq, N., Humayun, M. (2025).** Intrusion Detection in Smart Grids Using

Artificial Intelligence-Based Ensemble Modelling. PeerJ Computer Science, Vol. 11. DOI: 10.1007/s10586-024-04964-9.

33. **Qazi, E.U.H., Zia, T., Faheem, M.H. (2024).** Zero-Touch Network Security (ZTNS): A Network Intrusion Detection System Based on Deep Learning. IEEE Access, Vol. 12, pp. 141625–141641. DOI: 10.1109/access.2024. 3466470.
34. **Koca, M., Aydın, M.A., Sertbaş, A. (2021).** A New Distributed Anomaly Detection Approach for Log IDS Management Based on Deep Learning. Turkish Journal of Electrical Engineering and Computer Sciences, Vol. 29, No. 5, pp. 2486–2501. DOI: 10.3906/elk-2102-89.
35. **Hariharan, S., Jerusha, Y.A., Suganeshwari, G. (2025).** A Hybrid Deep Learning Model for Network Intrusion Detection System Using Seq2Seq and ConvLSTM-Subnets. IEEE Access, Vol. 13, pp. 30705–30722. DOI: 10.1109/access.2025.3541399.
36. **Althobaiti, M.M., Escorcia-Gutierrez, J. (2024).** Weighted Salp Swarm Algorithm with Deep Learning-Powered Cyber-Threat Detection for Robust Network Security. AIMS Mathematics, Vol. 9, No. 7, pp. 17676–17695. DOI: 10.3934/math.2024 859.
37. **Kaushik, S., Bhardwaj, A., Almogren, A. (2025).** Robust Machine Learning Based Intrusion Detection System Using Simple Statistical Techniques in Feature Selection. Scientific Reports, Vol. 15. DOI: 10.1038/s41598-025-88286-9.
38. **Othman, T.S., Abdullah, S.M. (2023).** Intrusion Detection Systems for IoT Attack Detection and Identification Using Intelligent Techniques. International Journal of Computer Networks and Applications, Vol. 10, No. 1, pp. 130–141. DOI: 10.22247/ijcna/2023/218517.
39. **Falowo, O.I., Botsyoe, L.E., Koshoedo, K. (2024).** Enhancing Cybersecurity with Artificial Immune Systems and General Intelligence: A New Frontier in Threat Detection and Response. IEEE Access, Vol. 12, pp. 123811–123829. DOI: 10.1109/access. 2024.3454543.
40. **Khayat, M., Barka, E., Serhani, M.A. (2025).** Reinforcement Learning with Deep Features: A Dynamic Approach for Intrusion Detection in IoT Networks. IEEE Access, Vol. 13, pp. 92319–92340. DOI: 10.1109/access.2025. 3569312.
41. **Hussain, S.F.M., Fathima, S.S.S. (2024).** Federated Learning-Assisted Coati Deep Learning-Based Model for Intrusion Detection in MANET. International Journal of Computational Intelligence Systems, Vol. 17. DOI: 10.1007/s44196-024-00590-w.
42. **Soltani, M., Khajavi, K., Siavoshani, M.J. (2024).** A Multi-Agent Adaptive Deep Learning Framework for Online Intrusion Detection. Cybersecurity, Vol. 7, No. 9. DOI: 10.1186/s42400-023-00199-0.
43. **Mohamed, D., Ismael, O. (2023).** Enhancement of an IoT Hybrid Intrusion Detection System Based on Fog-to-Cloud Computing. Journal of Cloud Computing, Vol. 12, No. 41, pp. 2–13. DOI: 10.1186/ s13677-023-00420-y.
44. **Çavuşoğlu, Ü. (2019).** A New Hybrid Approach for Intrusion Detection Using Machine Learning Methods. Applied Intelligence, Vol. 49, No. 8, pp. 1–18. DOI: 10.1007/s10489-018-01408-x.
45. **Agarwal, A., Sharma, P., Alshehri, M. (2021).** Classification Model for Accuracy and Intrusion Detection Using Machine Learning Approach. PeerJ Computer Science, Vol. 7. DOI: 10.7717/peerj-cs.437.
46. **Yang, J., Lim, H. (2021).** Deep Learning Approach for Detecting Malicious Activities over Encrypted Secure Channels. IEEE Access, Vol. 9, pp. 39229–39244. DOI: 10.1109/access.2021.3064561.
47. **Abdullah, M. (2024).** IoT-CDS: Internet of Things Cyberattack Detecting System Based on Deep Learning Models. CMC, Vol. 81, No. 3, pp. 4266–4290. DOI: 10.32604/cmc.2024.059271.
48. **Elsaid, S.A., Shehab, E., Mattar, A.M. (2024).** Hybrid Intrusion Detection Models Based on GWO Optimized Deep Learning. Discover Applied Sciences, Vol. 6, No. 531, pp. 1–22. DOI: 10.1007/ s42452-024-06209-1.
49. **Ahmed, U., Jiangbin, Z., Almogren, A. (2024).** Explainable AI-Based Innovative

Hybrid Ensemble Model for Intrusion Detection. Journal of Cloud Computing: Advances, Systems and Applications, Vol. 13, No. 150. DOI: 10.1186/s13677-024-00712-x.

50. **Zhao, W., Zhao, Z. (2024).** Providing a Hybrid Approach to Increase the Accuracy of Intrusion Detection Systems in Computer Networks. Journal of Engineering and Applied Science, Vol. 71, No. 123. DOI: 10.1186/s44147-024-00404-y.
51. **Logeswari, G., Bose, S., Anitha, T. (2023).** An Intrusion Detection System for SDN Using Machine Learning. Intelligent Automation & Soft Computing, Vol. 35, No. 1, pp. 867–880. DOI: 10.32604/iasc. 2023.026769.
52. **Alghamdi, R., Bellaiche, M. (2023).** An Ensemble Deep Learning Based IDS for IoT Using Lambda Architecture. Cybersecurity, Vol. 6, No. 5. DOI: 10.1186/s42400-022-00133-w.
53. **Pavithra, S., Vikas, K.V. (2024).** Detecting Unbalanced Network Traffic Intrusions with Deep Learning. IEEE Access, Vol. 12, pp. 74096–74112. DOI: 10.1109/access.2024. 3405187.
54. **Bella, K., Guezzaz, A., Benkirane, S. (2024).** An Efficient Intrusion Detection System for IoT Security Using CNN Decision Forest. PeerJ Computer Science, Vol. 10. DOI: 10.7717/peerj-cs.2290.
55. **Keshk, M., Koroniotis, N., Pham, N. (2023).** An Explainable Deep Learning-Enabled Intrusion Detection Framework in IoT Networks. Information Sciences, Vol. 639. DOI: 10.1016/j.ins.2023.119000.
56. **Vinayakumar, R., Alazab, M., Soman, K.P. (2019).** Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access, Vol. 7, pp. 41525–41550. DOI: 10.1109/access. 2019.2895334.
57. **Liu, L., Wang, P., Lin, J. (2021).** Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning. IEEE Access, Vol. 9, pp. 7549–7562. DOI: 10.1109/access.2020. 3048198.
58. **Megantara, A.A., Ahmad, T. (2021).** A Hybrid Machine Learning Method for Increasing the Performance of Network Intrusion Detection Systems. Journal of Big Data, Vol. 8, No. 142. DOI: 10.1186/s40537-021-00531-w.
59. **Aljuaid, W.H., Alshamrani, S.S. (2024).** A Deep Learning Approach for Intrusion Detection Systems in Cloud Computing Environments. Applied Sciences, Vol. 14, No. 13. DOI: 10.3390/app141 35381.
60. **Samy, A., Yu, H., Zhang, H. (2020).** Fog-Based Attack Detection Framework for Internet of Things Using Deep Learning. IEEE Access, Vol. 8, pp. 74571–74583. DOI: 10.1109/access.2020.2988854.
61. **Hnamte, V., Nhung-Nguyen, H., Hussain, J. (2023).** A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE. IEEE Access, Vol. 11, pp. 37131–37146. DOI: 10.1109/ access.2023.3266979.
62. **Kitchenham, B., Charters, S. (2007).** Guidelines for Performing Systematic Literature Reviews in Software Engineering.
63. **Kitchenham, B., Brereton, P. (2012).** A Systematic Review of Systematic Reviews in Software Engineering. Information and Software Technology, Vol. 54, No. 5, pp. 1–20.
64. **PRISMA (2025).** Preferred Reporting Items for Systematic Reviews and Meta-Analyses.
65. **Aparcana-Tasayco, A.J., Gamboa-Cruzado, J. (2022).** Machine Learning for Management in Software-Defined Networks: A Systematic Literature Review. IEIE Transactions on Smart Processing and Computing, Vol. 11, No. 6, pp. 400–411. DOI: 10.5573/ieiespc.2022.11.6. 400.
66. **Guembe, B., Misra, S., Azeta, A. (2025).** Bibliometric Analysis of Artificial Intelligence Cyberattack Detection Models. Artificial Intelligence Review, Vol. 58, No. 177. DOI: 10.1007/s10462-025-11167-0.
67. **de Azambuja, A.J.G., Plesker, C., Schützer, K. (2023).** Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0: A Survey. Electronics, Vol. 12, No. 1920. DOI: 10.3390/electronics 12081 920.
68. **Ofusori, L., Bokaba, T., Mhlongo, S. (2024).** Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction.

Applied Artificial Intelligence, Vol. 38, No. 1. DOI: 10.1080/08839514.2024.2439609.

69. **Albahri, O.S., AlAmoodi, A.H. (2023).** Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database. Mesopotamian Journal of CyberSecurity, pp. 158–169. DOI: 10.58496/mjcsc/ 2023/018.
70. **Lánský, J., Ali, S., Mohammadi, M. (2021).** Deep Learning-Based Intrusion Detection Systems: A Systematic Review. IEEE Access, Vol. 9, pp. 101574–101599. DOI: 10.1109/access.2021.3097 247.
71. **Valdivia, J.R., Gamboa-Cruzado, J., de Villa, P.D.L.C.V. (2023).** Systematic Literature Review on Machine Learning and Its Impact on APIs Deployment. Computación y Sistemas, Vol. 27, No. 4, pp. 1107–1124. DOI: 10.13053/cys-27-4-4371.
72. **Edje, E. (2024).** Anomaly-Based Intrusion Detection Techniques in Internet of Things Ecosystem: A Review. FUPRE Journal of Scientific and Industrial Research (FJSIR), Vol. 8, No. 4, pp. 352–372.
73. **Özgür, A., Erdem, H. (2016).** A Review of KDD99 Dataset Usage in Intrusion Detection and Machine Learning Between 2010 and 2015. Procedia Computer Science, Vol. 102, pp. 445–450. DOI: 10.7287/peerj.preprints. 1954v1.
74. **Arqane, A., Boutkhoum, O., Boukhriss, H. (2022).** Intrusion Detection System Using Ensemble Learning Approaches: A Systematic Literature Review. International Journal of Online & Biomedical Engineering, Vol. 18, No. 13, pp. 4–20. DOI: 10.3991/ijoe.v18i13.33519.
75. **Chinnasamy, R., Subramanian, M., Easwaramoorthy, S.V. (2025).** Deep Learning vs. Machine Learning for Network-Based Intrusion Detection: A Systematic Review. ICT Express, Vol. 11, No. 1, pp. 15–29. DOI: 10.1016/j.icte.2025. 01.005.
76. **Cárdenas-Quispe, A., Vergaray-Mezarina, R., Gamboa-Cruzado, J. (2021).** Machine learning para la detección de malware en Android: Revisión sistemática de la literatura. Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI), No. E45, pp. 318–331.
77. **Khalaf, B.A., Mostafa, S.A., Mustapha, A. (2019).** Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods. IEEE Access, Vol. 7, pp. 51691–51713. DOI: 10.1109/access. 2019.2908998.
78. **Bar, S., Prasad, P.W.C., Sayeed, M.S. (2024).** Enhancing Internet of Things Intrusion Detection Using Artificial Intelligence. Computers, Materials & Continua, Vol. 81, No. 1, pp. 1–23. DOI: 10.32604/cmc.2024. 053861.
79. **Padilla-Gomez, M., Gamboa-Cruzado, J., Távara-Aponte, S. (2024).** Systematic Literature Review on Cybersecurity and Its Influence on Cyber Attacks Targeting IoT Devices. Computación y Sistemas, Vol. 28, No. 4, pp. 1847–1864. DOI: 10.13053/cys-28-4-5006.
80. **Raimundo, R.J., Rosário, A.T. (2022).** Cybersecurity in the Internet of Things in Industrial Management. Applied Sciences, Vol. 12, No. 3. DOI: 10.20944/preprints202110. 0312.v1.
81. **Padilla, D.E.C., Fajardo-Toro, C.H., Riola, J. (2022).** Ciberseguridad y ciberdefensa marítima: análisis bibliométrico años 1990–2021. Revista Ibérica de Sistemas e Tecnologias de Informação, No. E49, pp. 197–210.
82. **Raimundo, R.J., Rosário, A.T. (2021).** The Impact of Artificial Intelligence on Data System Security: A Literature Review. Sensors, Vol. 21, No. 21. DOI: 10.3390/s21217029.
83. **Valdiviezo, M., Huillca, F., Alarcon, F. (2024).** Machine Learning in Cybersecurity: Systematic Literature Review. 22nd LACCEI International Multi-Conference for Engineering, Education, and Technology. DOI: 10.18687/laccei2024.1.1.723.
84. **Li, Y., Liu, Q. (2021).** A Comprehensive Review Study of Cyber-Attacks and Cybersecurity: Emerging Trends and Recent Developments. Energy Reports, Vol. 7, pp. 8176–8186. DOI: 10.1016/j.egyr.2021.08.126.
85. **Zhang, Z., Al Hamadi, H., Damiani, E. (2022).** Explainable Artificial Intelligence Applications

in Cyber Security: State-of-the-Art in Research. Center for Cyber-Physical Systems. DOI: 10.1109/ access.2022.3204051.

86. **Koca, M. (2025).** A Comprehensive Bibliometric Analysis of Big Data and Cyber Security: Intellectual Structure. Trends, and Global Collaborations, Knowledge and Information Systems. DOI: 10.21203/rs.3.rs-4616992/v1.
87. **Yılmaz, V. (2025).** A Bibliometric Analysis on Cybersecurity Using VOSviewer: An Evaluation for Public Security. Balkan Journal of Electrical and Computer Engineering, Vol. 13, No. 2, pp. 210–218. DOI: 10.17694/bajece.1608364.
88. **Judijanto, L., Endrianto, E., Vandika, A.Y. (2024).** Mapping the Cybersecurity Research through Bibliometric Analysis. West Science Information System and Technology, Vol. 2, No. 3, pp. 374–382. DOI: 10.58812/wsist.v2i03.1534.
89. **Goranin, N., Hora, S.K., Čenys, H.A. (2024).** A Bibliometric Review of Intrusion Detection Research in IoT: Evolution, Collaboration, and Emerging Trends. Electronics, Vol. 13, No. 16. DOI: 10.3390/electronics13163210.
90. **Satilmiş, H., Akleylek, S., Tok, Z.Y. (2024).** A Systematic Literature Review on Host-Based Intrusion Detection Systems. IEEE Access, Vol. 12, pp. 27237–27266. DOI: 10.1109/access.2024. 3367004.
91. **Alegre-Veliz, R., Gaspar-Ortiz, P., Gamboa-Cruzado, J. (2022).** Machine Learning for Feeling Analysis in Twitter Communications: A Case Study in HEYDRU!. Perú, International Journal of Interactive Mobile Technologies (iJIM), Vol. 16, No. 24, pp. 126–142. DOI: 10.3991/ijim.v16i24.35493.
92. **Villavicencio, H.E., Gamboa-Cruzado, J., López-Goycochea, J. (2024).** The Role of Artificial Intelligence in the Diagnosis of Neoplastic Diseases: A Systematic and Bibliometric Review. International Journal of Online and Biomedical Engineering (iJOE), Vol. 20, No. 4, pp. 43–68. DOI: 10.3991/ijoe.v20i04.45429.
93. **Espinoza-Ortega, M.G., Quevedo-Sacoto, A.S. (2025).** Impacto of Artificial Intelligence on Cybersecurity Processes in Industrial Security: A Narrative Literature Review. Revista Científica MQRInvestigar, Vol. 9, No. 1, pp. 1–19. DOI: 10.56048/mqr20225.9.1.2025.e68.

Article received on 25/03/2026; accepted on 16/07/2026.
**Corresponding author is Germán Rios-Toledo.*